Universidad Carlos III de Madrid
Escuela Politécnica Superior

PROYECTO FINAL DE CARRERA

Gestor de Certificados Digitales con PKI

Autor:
D. Francisco Javier Castro Martínez

Supervisor:
Dr. José René Fuentes Cortez

Memoria presentada para obtener el título de Ingeniero por la Universidad Carlos III de Madrid en el Programa de Ingeniería Técnica en Informática de Gestión

en el

Departamento de Informática

4 de noviembre de 2015

Proyecto Final de Carrera de presentado por el bachiller Francisco Javier Castro Martínez en el grupo COSEC (UC3M Computer Security Lab) del Departamento de Informática de la Universidad Carlos III de Madrid para la obtención del título de Ingeniero Técnico en Informática de Gestión por la Universidad Carlos III de Madrid en el Programa de Ingeniería Técnica en Informática de Gestíon.

Terminada en Madrid, el 22 de Octubre de 2015.

Título:
Gestor de Certificados Digitales con PKI

Bachiller:
Francisco Javier Castro Martínez

Director:
José René Fuentes Cortez
Departamento de Informática
Grupo de Investigación COSEC
Universidad Carlos III de Madrid
28911 Leganés, Madrid, España

Esta proyecto de fin de curso ha sido realizado dentro del grupo de investigación COSEC (UC3M Computer Security Lab) como parte de las actividades de investigación del grupo. Asimismo, el mismo trabajo final se ha realizado durante mi tiempo libre de mi trabajo en Canon España con el objetivo de concluirlo para la obtención del título de Ingeniero de Gestión por la Universidad Carlos III de Madrid en el Programa de Ingeniería de Gestión.

Este Trabajo de Final de Carrera está dedicado a mi pareja Anna.

Agradecimiento

En primer lugar quiero agradecer a mi tutor, José René por aceptar el llevar acabo mi proyecto fin de carrera y estar siempre disponible para cualquier cosa que necesitara haciendo dicho trabajo más llevadero y sin el cual no hubiera podido realizarlo.

En otro nivel de agradecimiento estarían mis padres, los cuales llevaban mucho tiempo esperando a que finalizara el interminable proyecto y siempre me han animado a que lo terminara.

Y por último, aunque el más importante agradecimiento es para Anna, que sin su apoyo incondicional y paciencia ha hecho posible que el proyecto llegue a buen puerto.

Resumen

Para la realización de este proyecto hemos tenido en cuenta los distintos sistemas criptográficos que existen en la actualidad que son la criptografía simétrica y asimétrica.

Estos primeros son muy rápidos y eficientes y se caracterizan por usar la misma clave para cifrar que para descifrar el mensaje que se quiere enviar y se llaman sistemas simétricos. Sin embargo, presentan varios problemas como es que necesitan un canal seguro para poder transmitir la clave, problema de distribución y gestión de claves. Además de no garantizar el no repudio.

Los segundos son los sistemas asimétricos o de clave pública que se caracterizan por la utilización de claves distintas para cifrar y descifrar. Lo que se cifra con una clave solo se puede descifrar con la otra. Cada usuario tiene un par de claves, una pública (que puede conocer todo el mundo) y una privada (que solamente conoce el propio usuario).

Con este sistema, dos usuarios que quieran intercambiar información lo hacen cifrando el mensaje a enviar con la clave pública del receptor. Por lo que al receptor le llega el mensaje cifrado y que sólo él puede descifrar utilizando su clave privada. Como esta clave privada sólo la conoce él, se resuelve el problema de distribución y gestión de claves del método anterior (simétrico) y sobre todo la confidencialidad del mensaje, ya que aunque alguien interceptara el mensaje cifrado no podría descifrarlo ya que no posee la clave privada del receptor. La clave pública se puede comunicar por un medio inseguro.

Otro elemento a utilizar es la función hash o resumen que surge para resolver el problema que tiene la criptografía asimétrica y es que es menos eficiente computacionalmente hablando que la simétrica a la hora de cifrar un mensaje. Por lo que se opta a coger un extracto o resumen del contenido a cifrar aplicándole un algoritmo. Este algoritmo se llama función hash y el resultado es la huella digital. Este resumen siempre va a tener la misma longitud independientemente del mensaje a resumir y cuya característica fundamental es que no es posible obtener el mensaje original a partir del resumen. Esta característica se llama unidireccional. Además es fácil y rápido de calcular. Y otra de las características fundamentales es que tiene un efecto avalancha y que consiste en que cualquier cambio por pequeño que sea en el mensaje a cifrar hace que el resumen sea totalmente diferente. Es decir, si se modifica un bit en el mensaje el resumen podría cambiar aproximadamente la mitad de sus bits. Y otra característica de las funciones resumen es que es prácticamente imposible que haya dos resúmenes iguales correspondiente a dos mensajes diferentes. Con estas características, es la función ideal para poder aplicarlo en la firma digital o electrónica. la comprobación de integridad de los ficheros o mensajes, autenticación de usuarios, etc.

Con estos elementos tendríamos resuelto los elementos básicos de seguridad que son la confidencialidad, autenticidad, integridad y no repudio. Pero podía surgir el problema de suplantación de identidad y que no sirva con el mero hecho de intercambiar las claves públicas entre los usuarios (como es el ataque de Man in the Midle). Para solventar este problema surgieron los certificados digitales, en los que además de la clave pública del usuario y su nombre tenemos una firma de una entidad de confianza, reconocida por ambas partes, que garantiza que dicha clave pública pertenece realmente al usuario que se identifica y por tanto se puede realizar la comunicación de una manera totalmente segura.

Esta entidad de confianza es lo que se denomina Autoridad de Certificación (AC) y forma parte de un sistema mayor que se denomina PKI (Public Key Infrastructure), que se encarga de la gestión de certificados.

Así pues aquí tenemos todos los elementos que van a formar parte de este proyecto de menor a mayor complejidad y que son:

Criptografía simétrica ⇒ criptografía asimétrica o de clave pública ⇒ firma digital ⇒ autoridad de certificación ⇒ certificados ⇒ PKI.

Palabras clave: Algoritmos, PKI (*Infraestructura de Clave Pública*), Clave Pública, Clave Privada, certificados digitales, firmas digitales, criptografía simétrica, criptografía asimétrica.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

1.1. Palabras Iniciales

Como situación de partida para la realización del proyecto nos encontramos con dos situaciones bien distintas.

1. ***Primer escenario:***

   La primera son los **certificados digitales** cuyo uso cada vez se está extendiendo más tanto en el ámbito profesional y laboral, por los empleados y trabajadores, como el personal, para hacer más seguras las transacciones con las administraciones públicas, empresas y sobre todo en el comercio Online.

   Este tipo de certificados hoy día es muy sencillo de obtener, y aunque requiere una serie de trámites administrativos, la mayor parte de la gente puede obtenerlos en poco tiempo y sin ningún coste asociado. No hay por tanto restricción tecnológica, ni económica para que una persona pueda solicitar un certificado, que le identificará de una manera segura en la red frente a otras personas u entidades.

   En España tenemos desde el año 2006 el DNI (Documento Nacional de Identidad) electrónico, que incluye un certificado de autenticación que sirve para identificar al titular de la tarjeta en una comunicación telemática y un certificado de firma que garantiza la integridad del documento firmado, la procedencia del documento y la autenticidad de origen.

   Pues bien con todo esto, su uso hasta el día de hoy ha sido muy escaso y apenas se ha aprovechado todo el potencial que en teoría tenía dicho documento. Las causas son muchas, entre otras son la necesidad de tener un lector de DNI electrónico para poder operar con él, la mala planificación y previsión en cuanto a su uso, la falta de información del uso del DNI-e, la crisis económica que frena las posibles, etc.

   Se suponía que la firma digital contenida en el chip del DNI electrónico, del que fuimos pioneros, iba a tener un uso masivo, pero desgraciadamente esto no ha sido así. Y no hemos sido capaces de conseguir promover la firma electrónica avanzada en nuestro país de la forma que queríamos. A pesar de tener una Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos y de un esquema nacional de

Seguridad aprobado por el decreto 3 de Enero de 2010.

2. ***Segundo escenario:***

   Y el segundo escenario es la **PKI (Public Key Infrastructure)**, que es un conjunto de aplicaciones y de servicios que nos permite utilizar la criptografía de clave pública (certificados) de forma fácil y efectiva. Pero que al contrario que los certificados digitales su implantación es muy costosa y es el mayor freno que tienen las empresas para poder implementarlo.

   La mayoría de las empresas optan por comprar la PKI debido a varias razones:

   - La tecnología PKI es relativamente compleja. La mayoría de los vendedores que ofrecen software PKI han invertido mucho en tecnología y el retorno de la inversión sólo es posible a través de múltiples ventas.
   - Una empresa que construya totalmente su PKI difícilmente podrá recuperar la inversión.
   - Dada la complejidad del software es improbable que la organización disponga de los recursos necesarios para el desarrollo.
   - Las patentes tienen un impacto en el coste del desarrollo.

   Debido a todas estas dificultades la mayoría de las empresas descartan la opción de construir su propia PKI .

   Por tanto, partiendo del escenario que tenemos actualmente, en el que los certificados cada vez tendrán un uso mayor y que implementar una PKI es muy costoso, como hemos visto en los puntos anteriores. Vamos a realizar un proyecto para la **gestión de certificados**, que englobe todo el ciclo de vida de dichos certificados así como la **implementación de una PKI** con los componentes básicos y su relación con los certificados. Aunque sea de una manera más simple, pero a la vez comprensible para el mayor número de personas. Comprender que una PKI es una solución global de seguridad, no un conjunto de soluciones puntuales diferentes, y que ofrece una única infraestructura de seguridad que puede ser usada por muchas aplicaciones en los entornos más heterogéneos. Específicamente, ofrece servicios de confidencialidad, integridad, autenticación y no repudio en numerosos contextos.

1.2. Motivación

La principal motivación para el desarrollo de este proyecto fin de carrera es el estudio en profundidad del funcionamiento de una infraestructura de clave pública y la importancia de los certificados en dicha infraestructura.

Para ellos estudiaremos y analizaremos todos los elementos que participan en dicha infraestructura, lo haremos de una manera didáctica y con ejemplo práctico para mostrar

cómo aplicarlo en una situación real. Esta situación real será una gestión documental segura de una empresa.

Es importante mencionar el estudio los certificados que son la base sobre la que se sustenta la infraestructura de clave pública. Con este estudio mostraremos de una manera clara y comprensible sus usos, aplicaciones, beneficios, ventajas y poner nuestro granito de arena para intentar que comprendiendo su funcionamiento promover e impulsar más su uso.

Lo que pretendemos realizar con este trabajo es mostrar el funcionamiento y aplicación de los certificados digitales para el cifrado y firma de documentos otorgándoles privacidad, autenticidad, integridad y no repudio. Esto lo realizan la mayoría de las aplicaciones del mercado a partir de un certificado dado.

Pero lo que nos diferencia de estas aplicaciones es que nosotros generaremos los propios certificados (a partir de la solicitud del usuario, previa verificación de su identidad) que se instalaran en las ordenadores de los usuarios. Y con la clave pública del usuario destinatario cifrará dicho documento. Además añadirá una firma del documento a cifrar, aplicando una función Hash a dicho documento.

Dicha infraestructura de clave pública (PKI) es muy costoso sobre todo por los recursos necesarios, formación, requerimientos técnicos, requerir una política de certificación que puede llegar a ser muy compleja tanto desde el punto de vista técnico como desde el punto de vista jurídico.

Si bien no vamos a desarrollar una AC globalmente reconocida o en un ámbito fuera de la empresa que lo utiliza, permite que los empleados/usuarios puedan fiarse unos de otros a pesar de no existir contacto físico y poder realizar intercambio de documentos con unas garantías de seguridad totales.

Al no existir un mercado suficientemente consolidado en PKI, las empresas que ofrecen este tipo de soluciones imponen unos precios altos, por lo que, asumir PKI como solución de seguridad, representa un alto costo económico para una organización. Igualmente PKI requiere un gran inversión de tiempo en diseño, implantación, pruebas y adaptación.

Además PKI presenta problemas de interoperabilidad, confianza y escalabilidad. Interoperabilidad ocasionada entre certificados generados por sistemas desarrollados por distintos fabricantes. Y el hecho de que se rijan por el estándar X.509 no garantiza que sean compatibles. La confianza entre AC de distintas organizaciones al no ser posible la verificación con éxito de cadenas de certificación si una AC raíz es no confiable. En cuanto a la escalabilidad cuando el número de certificados emitidos a los usuarios va creciendo, debido a que las listas de revocación en cada operación que involucre certificados y firmas digitales.

PKI es una solución compleja, lo que conduce a los usuarios finales a seguir utilizando los sistemas tradicionales de control y autenticación, basado en nombre y contraseña y listas de control de acceso.

Por todos estos motivos vamos a implementar una PKI básica donde poder comprender como funciona internamente y su relación con la aplicación de gestión de certificados y firmas digitales. Y tener integrado en una única solución un modelo completo de criptografía

de clave pública.

1.3. Objetivos

El principal objetivo del proyecto es la realización de una aplicación para la gestión documental segura de una empresa mediante el uso de certificados digitales y firmas digitales. Para ello implementaremos nuestra propia PKI (infraestructura de clave pública). Lo que nos permitirá cerrar el ciclo de vida de un certificado, desde que se solicita hasta que se revoca o expira. Por lo que se tendrá una visión más clara de la verdadera labor y función de los certificados, sus características y aplicaciones más frecuentes.

Para realizar el proyecto tendremos una aplicación que tendrá distintos roles en función del usuario que la vaya a utilizar y de lo se quiera realizar. Tendremos que diferenciar principalmente dos partes: la primera que simulará el funcionamiento de una pequeña PKI y por otro lado la que se encarga de gestionar el cifrado y firma de PDFs previamente generados. Para este cifrado y firma utilizaremos certificados digitales y así como la firma XADES (XML Advanced Electronic Signature), y estos certificados los habrá generado previamente la PKI .

En esta PKI tendremos que definir los elementos que la componen y que son:

- ***La autoridad de certificación:*** encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.
- ***La autoridad de registro (RA, Registration Authority):*** es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.
- ***Los repositorios:*** son las estructuras encargadas de almacenar la información relativa a la PKI . Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados. En una lista de revocación de certificados (o, en inglés, CRL, Certificate Revocation List) se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.
- ***La autoridad de validación (o, en inglés, VA, Validation Authority):*** es la encargada de comprobar la validez de los certificados digitales.
- ***Los usuarios y entidades finales*** son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI (para validar firmas digitales, cifrar documentos para otros usuarios, etc.)
- ***Servidor de certificados:*** componente encargado de expedir los certificados aprobados por la autoridad de registro. La generación de la clave pública para el usuario está formada por los datos del usuario y finalmente se firma digitalmente con la clave privada de la autoridad de certificación.

PKI CertiGes realizará la firma y cifrado de los documentos PDF una vez que se hayan generado, así como la verificación de firma y descifrado, y para que no puedan acceder

a estos ni modificar el contenido otros usuarios no autorizados. Cada usuario tendrá en su ordenador un certificado (emitido por la AC (Autoridad de Certificación) de la PKI) y que le permite poder visualizar los PDFs que se encuentran en el repositorio y que si no pertenecen a dicho usuario no podrían acceder al contenido. Además realizará las funciones típicas de una PKI .

Normalmente la seguridad de estos gestores documentales se basan en los permisos a los que tienen acceso dichos usuarios para poder gestionar los documentos PDFs o de cualquier otro tipo con los que trabajan. Nosotros pretendemos utilizar los certificados para dotarles a los documentos PDFs de esa seguridad de una manera implícita y transparente al usuario. Pero sin que ello signifique que sea menos seguro o implique un mayor grado de complejidad en la usabilidad de la aplicación.

1.4. Estructura de la memoria

La estructura de este Trabajo Final de Carrera es como sigue:

- El capítulo 1 es la introducción. Ahí se detalla los principales escenarios que aborda este trabajo. Por una parte se describen situaciones que dan lugar a la motivación de este Trabajo. Al final del mismo se describen los objetivos planteados en la realización de este Trabajo.
- El Capítulo 2 es el Estado del Arte de lo relacionado con la actualidad al respecto de las criptografía de certificados y firmas digitales. Se describen algunos conceptos básicos generales para la comprensión de este trabajo. Además, se mencionan firmas líderes en la rama, los aspectos fundamentales, procedimientos en la gestoría de certificados y firmas digitales.
- El capítulo 3 es donde se realiza el análisis de la solución que queremos desarrollar comenzando con el planteamiento del problema y la perspectiva general de la solución. A continuación se indica la arquitectura preliminar con la que vamos a trabajar, tanto de la PKI como de la solución completa. También indicaremos el estudio tecnológico utilizado para el desarrollo. Se muestran también los casos de usos extraídos del análisis así como el catálogo de requisitos software, tanto funcionales como no funcionales.
- En el capítulo 4 es donde se encuentra el modelo de datos que usaremos para la implementación junto con su diccionario de datos. Mostraremos también la definición de interfaces de usuario así como la arquitectura definitiva.
- El capítulo 5 exponen las conclusiones tras la realización del proyecto así como las futuras mejoras que se podrían aplicar al proyecto y las futuras líneas de actuación.
- Y por último se añade el anexo con la gestión del proyecto, con la planificación y seguimiento del proyecto. Además se incluye el presupuesto junto con las desviaciones detectadas.

Capítulo 2

Estado del Arte

2.1. Introducción

Para la realización del proyecto hemos optado por analizar el funcionamiento de los sistemas criptográficos que existen hoy día de criptografía asimétrica o también llamados sistemas de clave pública, al igual que las firmas digitales. Debido al aumento de documentos digitales y la cada vez menor emisión de documentos oficiales en papel impreso tanto de empresas privadas como de organismos oficiales hacen que cambie la seguridad que deben tener estos nuevos documentos electrónicos y que nos garanticen las mismas medidas que nos garantizaban los documentos en papel.

El proyecto a realizar que estamos presentando es un sistema basado en la **gestión de certificados y firmas digitales** para garantizar la integridad, confidencialidad, autenticidad y no repudio de los documentos (PDFs previamente generados) de la entidad. Estas características nos las proporciona la combinación de ambos elementos y la criptografía de clave pública.

Con el objetivo de describir las características específicas de la aplicación en cuestión, a continuación planteo de manera general los siguientes escenarios posibles para la implementación, uso etc. para la cual la presente aplicación puede ser considerada una herramienta útil:

2.1.1. Escenario 1. Empresa con características generales

En esta organización los documentos confidenciales serán las nóminas, datos fiscales, anticipos de nómina y demás documentación económica que un empleado tenga en la empresa y el funcionamiento general de la aplicación será:

"Con los documentos pdf, una vez generados, será la Autoridad de Certificación (AC) la que se encargará de cifrar su contenido con la clave pública del empleado/usuario al que va dirigido y además firmará el contenido de dicho pdf con la clave privada de la AC y se añadirá al documento cifrado. Después cada usuario, que tendrá instalado en su máquina su certificado, podrá visualizar los documentos que están cifrados de manera totalmente transparente. También podrá cada usuario cifrar y descifrar documentos para el intercambio de información segura entre empleados/usuarios del sistema."

La implementación de la herramienta es particularmente para uso exclusivo de una

intranet de la empresa, para lo cual una arquitectura de cliente-servidor es necesaria, además en este escenario no es necesario el acceso fuera de la intranet.

2.1.2. Escenario 2. Organización encargada con la manipulación de los datos de pacientes en hospitales, clínicas, centros ontológicos, etc.

Usualmente los datos y pruebas médicas de los pacientes de un Hospital, son documentos pdf que seguirán el mismo patrón que en el caso 1, salvo que habrá que añadir más medidas de seguridad para permitir conexiones remotas, mediante servidores seguros y que para identificarse sea necesario un certificado en la máquina desde la que se conecte. Además será necesaria una página web desde la que se acceda a dichos datos desde el exterior.

Y en el caso de que se utilizada una versión móvil, pues habría que añadir la seguridad específica para este tipo de dispositivos.

En este escenario, es necesaria la implementación de una aplicación web, ya que los pacientes deben poder consultar sus datos desde cualquier lugar. Hoy en día con el avance de la tecnología móvil, la misma aplicación web deberá tener su homologo para acceso vía móvil.

Además de una de estas dos opciones, también desarrollaremos una pequeña PKI (Public Key Infrastructure) ya que se trata de englobar una política de medidas que llevará a cabo una segura gestión documental. En primer lugar el sistema será capaz de **gestionar sus propios certificados digitales**. La intención es que muestre todo el proceso ó ciclo de vida de un certificado. Desde que se solicita la generación de dicho certificado digital, que lo solicitaría un empleado/usuario del sistema, hasta como se crea, como se gestiona y como se elimina o revoca dicho certificado a nivel local.

La finalidad de los certificados es el de resolver el problema de administrar las claves públicas y que la identidad del dueño no pueda ser falsificada. (la idea es que una tercera entidad intervenga en la administración de las claves públicas y asegure que las claves públicas tengan asociado un usuario claramente identificado, aquí es donde la tercera entidad entra en juego y sería nuestra propia AC (Autoridad de Certificación). Todo esto necesita también un marco jurídico que aclare las responsabilidades y un marco de estandarización que permita una compatibilidad y calidad de los productos usados.

Ya que la implementación una PKI como tal, estaría fuera del alcance de este trabajo, debido a su complejidad tanto técnica y de factores como: autoridad para autorización de políticas, políticas y procedimientos de seguridad, firewall, responsabilidades legales, OCSP(Online Certificate Protocol), entrenamiento a usuarios, procesos de revocación, administración del hardware, OIDs (Object Identifiers). Es decir, una infraestructura de clave pública (PKI) es la arquitectura, organización, tecnología, practicas, políticas y procedimientos que en conjunto soportan la implantación y operación de un sistema criptográfico de clave pública basado en certificados. De esto el 80 % son políticas y 20 % tecnología. [3]

La creación de esta pequeña PKI tiene un gran **sentido didáctico** para comprender sobre todo el porqué de los distintos componentes que la forman y la relación que tienen con el uso de los certificados una vez creados. Ya que la PKI utiliza la criptografía de clave pública y esa es la base de los certificados y firmas digitales. [30]

2.2. Criptografía: Conceptos Básicos

Comenzamos con la definición de Criptografía, [23] palabra viene del griego cripto (que significa “ocultar") y graphos (que significa “escribir"). La criptografía consiste en tomar el documento original y aplicarle un algoritmo cuyo resultado es un nuevo documento. Este documento está cifrado: no se puede entender nada al leerlo directamente. Podemos, tranquilamente, hacerlo llegar hasta el destinatario, que sabrá aplicar el algoritmo para recuperar el documento original.

Las claves son combinaciones de símbolos (letras, números, signos de puntuación, etc.). Por lo que la seguridad está expuesta a los ataques de fuerza bruta: que consiste en probar todas las combinaciones posibles de símbolos. Para paliar en lo posible este riesgo podemos hacer:

Utilizar claves de gran longitud (512-1024-2048-4096 bytes), de manera que el atacante necesite muchos recursos computacionales para cubrir el rango rápidamente.

Cambiar regularmente la clave. De esta forma, si alguien quiere intentar cubrir todo el rango de valores, le limitaremos el tiempo para hacerlo.

Utilizar todos los tipos de caracteres posibles: ya que por ejemplo una clave compuesta sólo de números (con diez valores posibles) es más fácil de adivinar que con números y letras (36 valores posibles).

No utilizar palabras fácilmente identificables: palabras de diccionario, nombres propios, etc.

Detectar repetidos intentos fallidos en un corto intervalo de tiempo. Por ejemplo, la tarjeta SIM del móvil se bloquea si fallamos tres veces al introducir el PIN:

Si un atacante consigue interceptar el mensaje enviado, al estar cifrado, no sería capaz de leer los datos que están protegidos mediante un algoritmo criptográfico o de cifrado.

Además de ser utilizada para ocultar el significado de los datos, la criptografía realiza otras necesidades críticas de seguridad para la transmisión de datos, como por ejemplo [19]:

1. Autentificar que el remitente de un mensaje es el auténtico remitente y no un impostor. Además permite probar que un usuario ha enviado un mensaje o realizar una acción determinada. Permite la generación de Certificados Digitales, sobre los cuales se basa el esquema de seguridad de una Infraestructura de Clave Pública (PKI). [30]
2. Garantizar la confidencialidad, ya que sólo un lector con el algoritmo de descifrado correcto puede leer el mensaje cifrado.
3. Proteger la integridad de la información, garantizando que los mensajes enviados no han sido alterados durante la transmisión.

2.2.1. Criptografía simétrica

Son sistemas criptográficos también llamados de clave única o de clave secreta porque utilizan la misma clave tanto para cifrar como para descifrar un mensaje. Para que pueda

funcionar correctamente, la clave debe estar mantenida en secreto por parte del emisor y del receptor del mensaje. Si la clave cae en manos de un tercero, el sistema deja de ser seguro, lo que implica desechar la clave y generar una nueva.

Generalmente este algoritmo es de conocimiento público y la fortaleza del algoritmo dependerá de la complejidad interna de dicho algoritmo así como de la longitud de la clave empleada. De ahí la importancia de elegir una clave adecuada. Y como hemos dicho antes las claves secretas son compartidas. Es el método que solemos identificar con la criptografía.

Los algoritmos de clave simétrica más utilizados han sido hasta hace poco DES (Digital Encryption Standard) y su versión extendida, Triple-DES (3-DES), viéndose ahora reemplazados por AES (Advanced Encryption Standard) . [19]

Los algoritmos de clave simétrica son en general, más sencillos y rápidos que los de clave asimétrica, pero su principal inconveniente es que implica que tanto el emisor como el receptor del mensaje tienen que intercambiar la clave simétrica de una forma segura. Esto se agrava mucho más cuando aumenta de manera considerable el número de interlocutores lo que conlleva al "Problema de distribución de claves".

Sin embargo, cuando el número de usuarios se reduce a una sola persona, el problema de la gestión de claves y la necesidad de comunicar la clave a nadie más desaparece. Por lo que una de sus utilidades sea el cifrado de archivos individuales o incluso el disco duro completo.

2.2.2. Criptografía asimétrica

Criptografía que se basa en el empleo de algoritmos de clave pública que usan distintas claves para cifrar y descifrar los mensajes. También se llama Criptografía de Clave Pública (CCP) ó PKI (Public Key Infrastructure) por sus siglas en inglés. Fue inventada en el año 1976 por los matemáticos Whit Diffie y Martin Hellman y es la base de la criptografía moderna. [30]

La criptografía asimétrica utiliza dos claves complementarias llamadas Clave Privada y Clave Pública. Las clave pública y privada están relacionadas matemáticamente entre sí. Siendo una la inversa de la otra. Las operaciones de cifrado y descifrado son compatibles e independientes del orden en que se aplican. [24] Se basan en mecanismos de una sola dirección, en los que es muy fácil ir en una dirección pero prácticamente imposible volver.

Las claves privadas deben ser conocidas únicamente por su propietario, mientras que la correspondiente clave pública como su nombre indica puede ser de conocimiento público.

Este tipo de criptografía está basada en la utilización de números primos muy grandes. Al multiplicar entre sí dos números primos muy grandes, el resultado obtenido no puede descomponerse eficazmente.

Es decir, incluso utilizando ordenadores muy avanzados y métodos aritméticos muy avanzados, sería casi imposible. Cabe resaltar que este proceso será más seguro cuanto mayor sea el tamaño de los números primos utilizados [19].

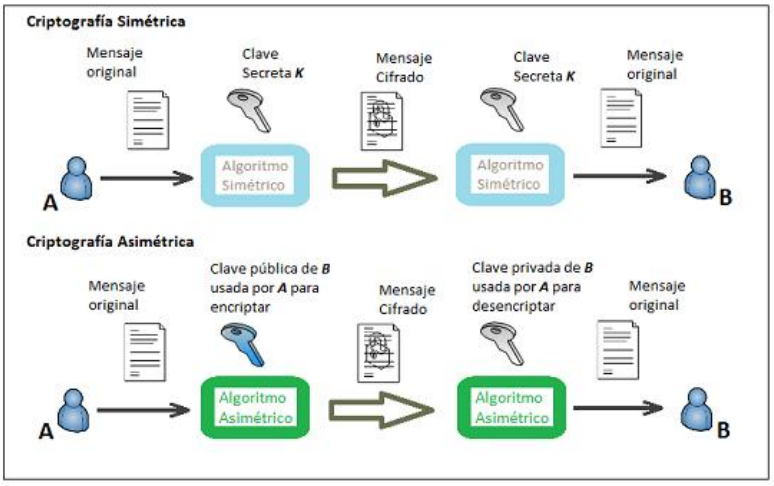


Figura 2.1: Criptografía Simétrica y Asimétrica

El problema que presentan los algoritmos de claves simétricas es que cuando el mensaje a cifrar es muy largo, el proceso de cifrar es muy lento.

Los usos más frecuentes de la criptografía de clave pública son [19]:

- **Cifrado:** El emisor cifra un mensaje con la clave pública del receptor.
- **Firma Digital:** Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.
- **Intercambio de claves:** como método seguro para intercambio de claves y poder utilizar un cifrado simétrico.

En el cuadro 2.1. se describen los diferentes usos de las claves dependiendo de la misma necesidad ya sean en la transmisión o recepción de un mensaje o servicio.

Tabla 2.1: Cuadro resumen de la criptografía asimétrica

Función	**Tipo de Clave:**	**La clave del:**
Cifrar datos para un receptor	Pública	Receptor
Firmar Datos	Privada	Emisor
Descifrar datos recibidos	Privada	Receptor
Verificar una firma	Publica	Emisor

2.3. El certificado Digital

La definición de certificado digital que tenemos en el BOE es [1], según la Ley 59/2003, de 19 de diciembre, de firma electrónica, artículo 6, un certificado digital es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos

datos de verificación de firma a un firmante y confirma su identidad.

Lo que convierte una firma electrónica avanzada, en una firma electrónica reconocida es el hecho de incorporar un certificado digital emitido por una Autoridad de Certificación legalmente constituida y a su vez reconocida, que garantiza que el sistema de generación del certificado cumple con los requisitos de seguridad necesarios. [24]

Un Certificado Digital consta de una pareja de claves criptográficas, una pública y una privada, creadas con un algoritmo matemático, de forma que aquello que se cifra con una de las claves sólo se puede descifrar con su clave pareja.

El certificado digital o certificado de clave pública es la base de lo que se conoce como infraestructura de clave pública. Éste consta de tres partes básicas que son: una identificación de usuario, el valor de la clave pública de este usuario y la firma de las dos partes anteriores. [16]

El certificado digital permite cifrar las comunicaciones. Solamente el destinatario de la información podrá acceder al contenido de la misma.

El titular del certificado debe mantener bajo su poder la clave privada, ya que si ésta es sustraída, el sustractor podría suplantar la identidad del titular en la red. En este caso el titular debe revocar el certificado lo antes posible, igual que se anula una tarjeta de crédito sustraída.

Otra definición de certificado digital es que es [15] un documento identificativo, que vincula a una persona o equipo con una clave pública, la cual a su vez está matemáticamente relacionada con una clave privada. La clave pública se emplea para el cifrado de información y la verificación de la firma digital, mientras que la clave privada se utiliza para realizar las operaciones opuestas.

El Certificado Digital es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet. Se trata de un requisito indispensable para que las instituciones puedan ofrecer servicios seguros a través de Internet. [5]

Como se muestra en [5] el certificado digital permite la firma electrónica de documentos. El receptor de un documento firmado puede tener la seguridad de que éste es el original y no ha sido manipulado y el autor de la firma electrónica no podrá negar la autoría de esta firma.

En el certificado digital se trata de una información que permite: [25]

- Identificarnos electrónicamente.
- Firmar documentos electrónicos con el mismo valor que la firma manuscrita.
- Cifrar documentos electrónicos, garantizando que estos datos no puedan ser vistos ni manipulados por terceras personas.

La clave pública forma parte de lo que se denomina Certificado Digital en sí, que es un documento digital que contiene la clave pública junto con los datos del titular, todo

ello firmado electrónicamente por una Autoridad de Certificación, que es una tercera entidad de confianza que asegura que la clave pública se corresponde con los datos del titular.

La Firma Electrónica sólo puede realizarse con la clave privada.

El certificado emitido garantiza que la AC ha verificado y confía plenamente en la identidad de la persona a la que pertenece. La AC manifiesta esta conformidad firmando el certificado y adjuntando dicha firma al final del mismo certificado.

La Autoridad de Certificación (AC) se encarga de emitir los certificados para los titulares tras comprobar su identidad. El certificado emitido garantiza que la AC ha verificado y confía plenamente en la identidad de la persona a la que pertenece. La AC manifiesta esta conformidad firmando el certificado y adjuntando dicha firma al final del mismo certificado.

Otro documento que suele firmar la AC es la Lista de Revocación de Certificados (CRL).

El formato de los Certificados Digitales está definido por el estándar internacional ITU-T X.509. De esta forma, los certificados pueden ser leídos o escritos por cualquier aplicación que cumpla con el mencionado estándar.

Existen varios tipos de certificados digitales, entre los cuales tenemos:
– *X.509 ICs (Identity Certificate)*
– *Certificados SPKI*
– *Certificados PGP*
– *AC s (Attribute Certificates)*

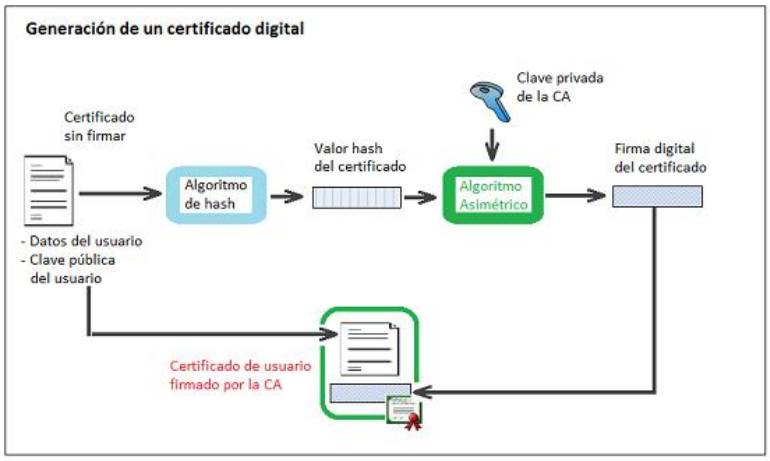


Figura 2.2: Generación de un Certificado Digital

Por tanto, un certificado es un documento electrónico que:

- asocia una identidad con su clave pública y
- la veracidad de esa asociación la garantiza la AC o PSC:
    - FNMT (Fabrica Nacional de Moneda y Timbre)

- Dirección General de la Policía (DNIe)
- Camerfirma, CatCert, Izenpe, AC CV...
- Registradores, Notarios...
- Etc.

2.3.1. Certificados X.509

En la realización del proyecto será uno de los tipos de certificados con los que trabajaremos.

Como podemos leer en [19] los Certificados X.509 son uno de los tipos de certificados cuyo uso está más extendido a lo largo de Internet. Su principal función es la de asociar una clave pública con una identidad determinada.

Actualmente, existen tres versiones de Certificados X.509:

- La versión 1 ha estado disponible desde 1988. Está ampliamente desplegada y es la más genérica.
- La versión 2 introduce el concepto de Identificadores únicos para el Sujeto (Subject) y para el Emisor (Issuer) del certificado, de manera que se pueda manejar la posibilidad de reutilizar los nombres del Emisor y del Sujeto a lo largo del tiempo. Sin embargo, como la mayoría de certificados recomiendan no reutilizar estos nombres, esta versión no es muy utilizada.
- La versión 3 es la más reciente, apareció en 1996 y soporta la noción de extensiones, lo que permite definir información adicional e incluirla en el campo Extensión del cuerpo del certificado.

En la implementación de la aplicación utilizaremos los certificados X.509 versión 3.

Como se describe en [19] todos los Certificados X.509 deben tener la siguiente información, además de la firma digital:

- **Version** (versión): Identifica la versión del estándar X.509 aplicado al certificado, lo cual afecta al tipo de información que pueda estar contenida en él. Generalmente será la versión 3.
- **Serial number** (número de serie): La entidad que crea el certificado es responsable de asignar un número de serie para distinguir a ese certificado de los otros que haya emitido dicha entidad. Cada certificado emitido por una AC debe tener un número de serie único.
- **Signature Algorithm** (algoritmo de la firma): Identifica el algoritmo asimétrico utilizado por el emisor para firmar el certificado.
- **Issuer Name** (Nombre del emisor): El DN del emisor. Identifica la AC que ha firmado y emitido el certificado.
- **Validity Period** (periodo de validez): Tiempo durante el cual el certificado es válido y la AC está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.

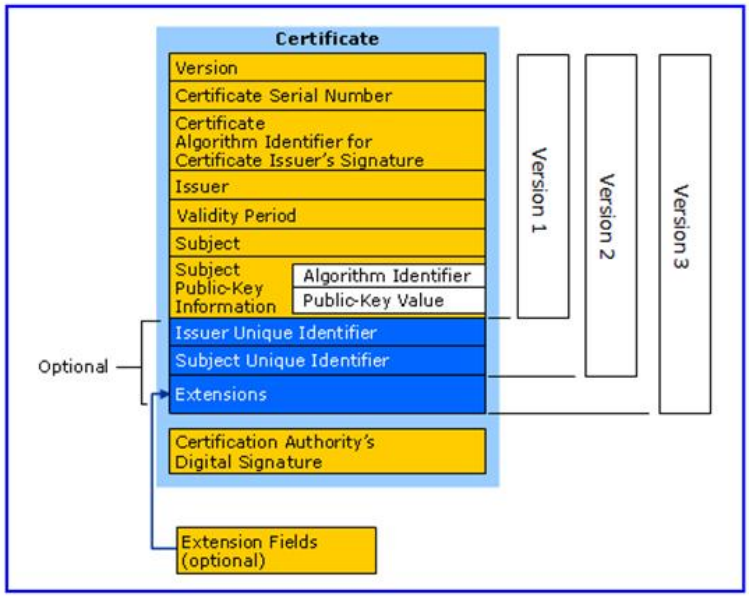


Figura 2.3: Estructura de un Certificado Digital [1]

- **Subject Name** (nombre del sujeto) El DNI de la entidad a la cual la clave pública del certificado referencia.

- **Subject Public Key Information** (Clave pública del sujeto): Es la clave pública de la entidad que está siendo identificada en el Certificado, junto al identificador del algoritmo que especifica qué algoritmo de encriptación se utiliza para encriptar esta clave, además de cualquier otro parámetro o información que pueda estar asociado a la clave pública.

- **Extensions** Limitaciones en el uso de la clave, indicación de que el sujeto es a su vez AC , etc.

- **Digital Signature (Firma Digital)**: es la firma digital de los datos del certificado con la clave privada de la autoridad certificadora AC .

Figura 2.4: Certificado X.509 (ejemplo abreviado) [13]

2.3.2. Firma Digital

La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación. Ofrece el soporte para la autenticación e integridad de los datos así como para el no repudio en origen, ya que el creador de un mensaje firmado digitalmente no puede argumentar que no lo es. [12]

Esta firma digital es imposible de falsificar a no ser que se descubra la clave privada del firmante.

Se basa en la propiedad de que en un mensaje cifrado utilizando la clave privada de un usuario sólo puede ser descifrado utilizando la clave pública asociada. Además se tiene la seguridad de que el mensaje que se ha descifrado utilizando la clave pública sólo pudo cifrarse utilizando la clave privada. Aquí se utiliza la clave privada para cifrar en lugar de la pública como se hacía con la criptografía de clave asimétrica.

Pero el principal inconveniente de los algoritmos de clave pública es la lentitud, que aumenta con el tamaño del mensaje a cifrar. [12]

Para evitar este problema, la firma digital hace uso de funciones hash (o resumen). Que es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, de tamaño fijo e independiente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, por lo que es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen hash idéntico.

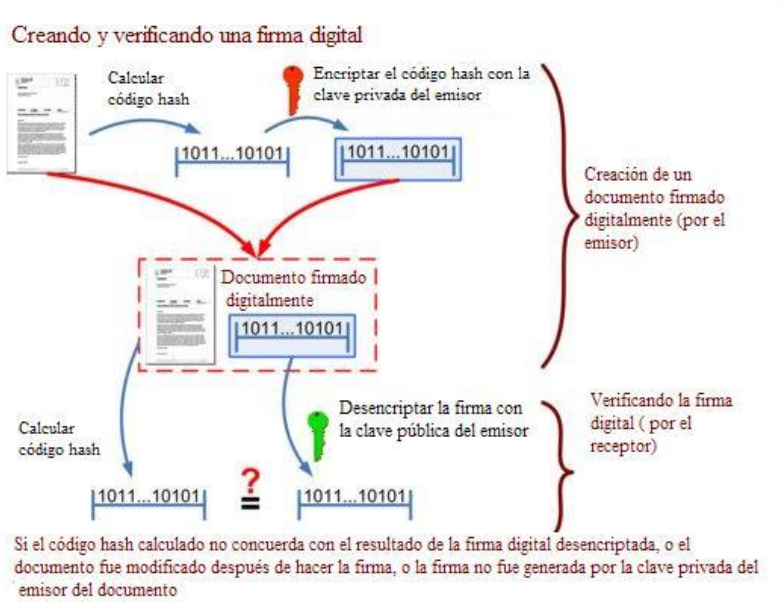


Figura 2.5: Creación y Verificación de una Firma Digital

Los algoritmos has más conocidos actualmente son los Message Digest (siendo el más usado el Message Digest 5 ó MD5 y los Secure Hash Algorithm (siendo el más usado el SHA-1). [19]

El primer paso es obtener el valor hash del mensaje y en el segundo paso el firmante debe utilizar su clave privada para encriptar este valor hash, a estos dos pasos se les conoce como firmar digitalmente un mensaje y al resultado obtenido como firma digital.

La verificación de la firma digital implica que otra persona desencripte la firma digital utilizando la clave pública del firmante. Si la puede desencriptar correctamente puede confiar en que el firmante realmente firmó el mensaje utilizando su clave privada. El resultado de la verificación es lo que se encriptó con la clave privada, en este caso el valor hash del mensaje. Si además el verificador tiene una copia del mensaje original en su poder, puede calcular el valor hash del mensaje y compararlo con lo obtenido en la desencriptación. Si los valores son iguales entonces puede confiar en que el mensaje que tiene es el mismo que el que recibió firmado. [19]

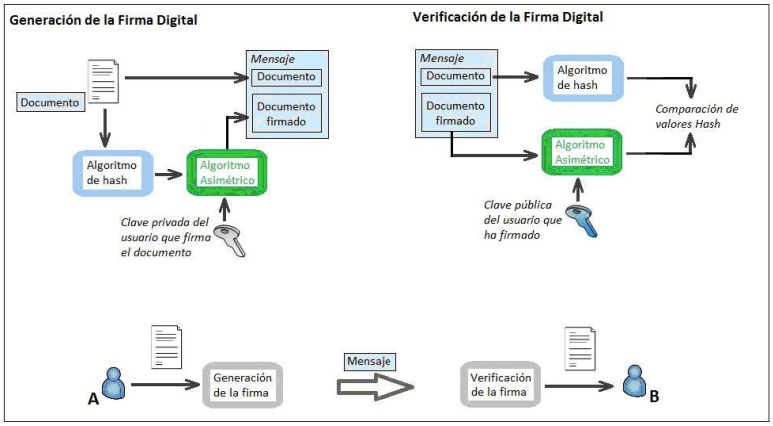


Figura 2.6: Generación y Verificación de una Firma Digital

2.3.3. DNI Electrónico (DNI-e)

El DNI electrónico es un certificado digital reconocido, que podrá ser utilizado para firmar documentos en las plataformas electrónicas [29].

El mismo DNIe es un Dispositivo Seguro de Creación de Firma por lo que las firmas generadas mediante el DNIe, son Firmas electrónicas reconocidas [29].

Otra definición de DNI es [22] que acredita física y electrónicamente la identidad y permite la firma electrónica de documentos.

Un Certificado de Identidad establece una asociación entre un nombre, denominado Distinguished Name ()DN) y la clave pública del usuario. [19]

2.4. Infraestructura de Clave Pública (PKI)

La infraestructura de clave pública (PKI) se puede definir [2] como el conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, administrar, almacenar, distribuir y revocar certificados de clave pública basados en criptografía de clave pública. [2]

Una infraestructura de Clave Pública es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública. [12]

2.4.1. Características de una PKI

Las infraestructuras de clave pública tienen en cuenta cuatro aspectos fundamentales en cualquier comunicación electrónica, estos son especialmente importantes si se habla de una transacción electrónica: [30]

- **Confidencialidad**: Una comunicación entre dos personas no debe ser vista ni interferida por una tercera persona que no forme parte de la comunicación. La tecnología

PKI usa la encriptación para asegurar la confidencialidad de los datos críticos que se encuentran en tránsito en la comunicación actual. También ofrece la posibilidad de encriptar datos valiosos almacenados en los servidores que tienen que conectarse a Internet, esto es importante porque si estos datos llegaran a ser interceptados, el atacante aún tendría que romper la encriptación antes de que pueda sacar ventaja de los mismos.

- **Autenticación**: Significa que el acceso a una comunicación electrónica debe estar restringido solo a quienes puedan presentar las credenciales necesarias de identidad. La forma más común de acreditar la identidad es a través de un identificador de usuario y una contraseña. Esta forma está considerada como un bajo nivel de autenticación y es frecuentemente fácil de romper. La tecnología PKI utiliza el certificado digital como credencial de identificación.
- **Integridad**: Los datos recibidos deben ser los mismos que los datos enviados, esto quiere decir que no deben haber sido modificados durante su transmisión ya sea por error o a propósito. La tecnología PKI utiliza los algoritmos hash para asegurar la integridad de estos datos. Las características de estos algoritmos hacen que cualquier cambio producido en el mensaje original durante su transmisión por la red se detecte como una pérdida de integridad. Normalmente se envía el mensaje y el valor de su hash, el receptor calcula el hash del mensaje recibido y lo compara con el valor del hash que le envió el transmisor, si los valores son idénticos se puede asegurar que el mensaje no ha sido modificado.
- **No-repudio**: Significa que si surge una discrepancia sobre lo que sucedió en una comunicación electrónica que implica intercambio de datos, habrá innegable evidencia presente dentro del sistema de comunicación que pueda ser utilizada para probar con suficiente certeza lo que realmente sucedió. Esto es especialmente sensible en operaciones que implican la firma de contratos electrónicos, en las cuales se evitaría que cualquiera de las partes que están implicadas en el contrato repudie lo que ha firmado. La tecnología PKI provee no-repudio a través del uso de la firma digital.

2.4.2. Funcionamiento básico de una PKI

El emisor (Juan) quiere comunicarse de manera segura con el receptor (Ana). Esto quiere decir que Juan no quiere que nadie más escuche esta conversación, quiere que la información enviada a Ana no sea alterada durante su transmisión y finalmente le gustaría disponer de algún mecanismo que pueda probar que ellos tuvieron esta conversación, en caso que Ana por algún motivo quiera negarlo. Esto lo vamos a explicar gráficamente como muestra la figura 2.7.

1. Juan crea una clave pública y una privada utilizando un algoritmo de clave pública. Luego, crea una solicitud de certificado, lo cual es el certificado justo antes de ser firmado por la Autoridad de Certificación. Ana envía su solicitud de certificado a la Autoridad de Registro (RA, Registration Authority) para ser firmado.
2. Cualquier acción de aprobación o desaprobación tiene lugar en la RA . Luego, la RA envía una solicitud a la AC para aprobación de políticas y para ser firmado.
3. El resultado de la firma del certificado es enviado de vuelta a Juan a través de la RA o es almacenada temporalmente en un repositorio.

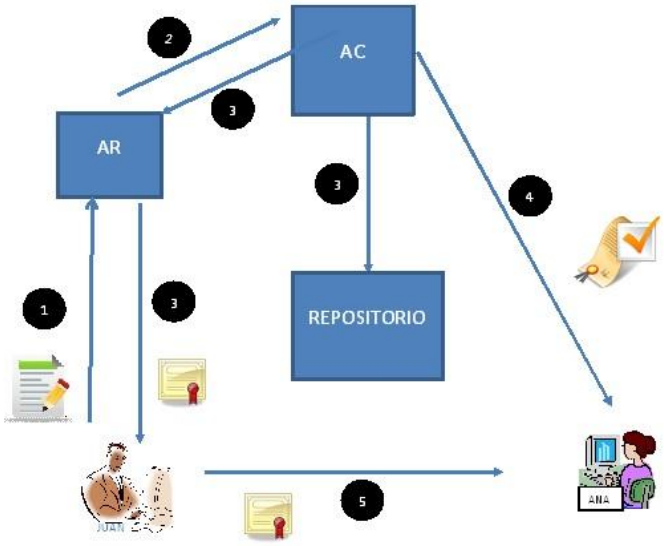


Figura 2.7: Uso del Certificado en transacciones seguras

4. Juan puede anunciar que su clave pública es confiable. Ana, que quiere comunicarse con Juan, pregunta por su certificado. Ana, para poder verificar el certificado de Juan, obtiene la clave pública de la AC que firmó la clave pública de Juan.
   Ana necesita hacerlo de manera segura. Si ambos están en la misma AC Ana ya tendrá la clave pública de dicha AC . En caso contrario, Ana solicitará a su AC que contacte a la AC de Juan para obtener su clave pública.
5. Finalmente, teniendo tanto Juan como Ana las claves públicas de ambos, pueden comunicarse de manera segura.

Finalmente, teniendo tanto el emisor como el receptor las claves públicas de ambos, pueden comunicarse de manera segura.

2.4.3. Infraestructura de Clave Pública

La PKI estaría formada por: [30]

- **La autoridad de certificación (AC)** encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.
- **La autoridad de registro (RA , Registration Authority)**: es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.
- **Los repositorios**: son las estructuras encargadas de almacenar la información relativa a la PKI . Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados. En una lista de revocación de certificados (CRL, Certificate Revocation List) se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.

- **La autoridad de validación (VA, Validation Authority)**: es la encargada de comprobar la validez de los certificados digitales.
- **La autoridad de sellado de tiempo (TSA, TimeStamp Authority)**: es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo. Esta última no será implementada.
- **Los usuarios y entidades finales** son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI (para validar firmas digitales, cifrar documentos para otros usuarios, etc.)
- **Servidor de certificados**: componente encargado de expedir los certificados aprobados por la autoridad de registro. La generación de la clave pública para el usuario está formada por los datos del usuario y finalmente se firma digitalmente con la clave privada de la autoridad de certificación.

Los certificados digitales son una parte fundamental de la tecnología PKI . Y un subconjunto de estos es PKIX que se refiere a la infraestructura de clave pública basada en certificados X.509 (Public Key Infraestructure X.509) y el termino certificado PKIX generalmente hace referencia a los perfiles de certificado y de lista de revocación basados en el estándar de certificados X.509v3.

Los elementos fundamentales que lo componen son: [30]

- **textitEntidad final (End Entity)**: Es el nombre genérico que reciben los usuarios de una PKI o los dispositivos que forman parte de ella, como enrutadores o servidores. Estos pueden ser identificados en el campo que define al propietario del certificado X.509. Las entidades usuarios normalmente utilizan los servicios que ofrece la PKI y los dispositivos normalmente los soportan.
- **textitAutoridad de Certificación (AC)**: Es la autoridad encargada de emitir los certificados digitales X.509 y usualmente también las Listas de Revocación de Certificados (CRLs), aunque a veces delega la función de emitir CRLs a un elemento denominado Emisor de CRL . También puede desempeñar funciones administrativas como las de registro de entidades finales o publicación de certificados, aunque normalmente estas funciones son desempeñadas por las autoridades de registro.
- **textitAutoridad de Registro (RA)**: Es un elemento opcional de la arquitectura PKIX que puede asumir algunas funciones administrativas de la AC , tal vez la más común sea el proceso de registro de las entidades finales, pero también puede realizar otras funciones como el proceso de revocación de certificados y el manejo de los datos de la entidad final.
- **textitEmisor de CRLs (CRL Issuer)**: Es un elemento opcional de la arquitectura PKIX al que la AC puede delegar la función de emitir las CRLs . Algunas veces se encuentra integrado en la AC a modo de servicio.
- **textitRepositorio (Repository)**: Es el término que hace referencia a cualquier método existente para almacenar certificados y CRLs , y así poder ser obtenidos por las entidades finales. Uno de estos métodos es el protocolo LDAP.

La figura 8 muestra los componentes de una PKI típica y sus relaciones:

Figura 2.8: Componentes de una PKI y sus relaciones

2.4.4. Descripción de todo lo que está hecho

En primer lugar, la forma más básica de proteger un documento PDF es ponerle una contraseña para evitar el acceso a personas que no conozcan dicha contraseña. Esto es algo que ofrecen casi todos los lectores de PDF, Microsoft Office y que si bien ofrece privacidad, no se puede considerar como un elemento a estudiar como sistema de seguridad.

También existen multitud de herramientas comerciales con mayor grado de seguridad para firmar documentos:

- **PDF Creator** ⇒ [4] Funciona mediante las ya clásicas impresoras virtuales, instala una impresora virtual en tu equipo, y cada vez que selecciones esta impresora al imprimir algo, creará un archivo PDF con el contenido a imprimir.

- **DigiSigner** ⇒ [6] Además de permitir firmar documentos PDF con tu certificado digital, también puedes utilizarlo como visor básico de documentos PDF. Permite insertar una marca de agua, así como un sellado de tiempo o realizar un procesamiento por lotes para firmar varios archivos PDF de una sola vez y es multiplataforma.
- **Sinadura** ⇒ [27] aplicación multiplataforma que permite firmar documentos de cualquier formato. Es un proyecto español de software libre que fue desarrollado para fomentar su uso en plataformas GNU/Linux y facilitar la gestión digital de documentos firmados.

  El programa permite, desde una interfaz muy sencilla, firmar varios documentos de una sola vez y realizar múltiples operaciones comunes, como sellado de tiempo, validaciones u otras.
- **JSignPdf** ⇒ [17] puede ser una aplicación sencilla para usuarios ofimáticos o una aplicación avanzada para usuarios con conocimientos sobre seguridad y firmas digitales, puesto que permite, mediante una casilla Advanced view, pasar de una a otra modalidad.
  En la modalidad básica, basta con seleccionar el almacén de certificados, el documento original, donde guardaremos el documento firmado, y algunos datos opcionales para

la firma. También se puede configurar de forma visible la marca de agua, con varios parámetros de diseño.

La versión avanzada incorpora todo tipo de opciones: cargar alias de certificados, realizar cifrados, certificaciones, selección de algoritmo hash y un largo etcétera.

- **Firmador de Escritorio** ⇒ [11] aplicación de escritorio muy sencilla para firmar archivos PDF que permite firmar documentos PDF en apenas tres clics. Es gratuito y está basado en java, lo que lo hace multiplataforma. Es muy cómodo y es ideal para usuarios poco familiarizados con los, generalmente, complejos pasos y conceptos de seguridad de los certificados digitales.
- **iSafePDF** ⇒ [14] A pesar de ser un programa feo y tosco para firmar PDF con certificado digital funciona bastante bien. Basta con seleccionar el archivo a firmar, el certificado digital en cuestión y pulsar el botón Process para realizar la firma. El programa es bastante simple y muy intuitivo, permitiendo de forma opcional cifrar con contraseña establecer protecciones (permitir o prohibir imprimir, copiar, etc...), así como establecer un sellado de tiempo o metadatos.
- **XolidoSign** ⇒ [31] Es uno de los programas con una interfaz más cuidada y apta para usuarios nóveles es Xolido Sign. Entre su funcionalidad básica, se encuentra la firma de archivos de cualquier tipo, el sellado de tiempo o la verificación de firmas.
- **EcoFirma** ⇒ [7] El Ministerio de Industria, Energía y Turismo desarrolló una interesante aplicación llamada EcoFirma, que permite firmar documentos de cualquier tipo, validar firmas o crear nuevas firmas.

  Permite proteger documentos con una contraseña con tu clave pública del certificado digital, y que sólo el autor pueda leer los documentos (con su clave privada), calcular huella del fichero (MD5, SHA1, SHA2, etc...), así como varias opciones interesantes. También permite sellado de tiempo, utilización de la familia XAdES para el tipo de firma, y varias opciones más. Funciona mediante Java, por lo que es multiplataforma y puede utilizarse tanto en Windows, GNU/Linux como Mac.
- **PDF Sign** ⇒ [26] versión para firmar PDF con certificado digital desde línea de comandos. Permite especificar ciertos parámetros para determinar los archivos a firmar, personalizar la firma, utilizar certificados digitales u otras opciones. Ideal para la creación de scripts o programas que automaticen las tareas. Disponible sólo para plataformas Windows.
- **PortableSigner** ⇒ [21] Similar a PDFSign pero multiplataforma. Desarrollado en Java.
- **LibreOffice** ⇒ [18] suite LibreOffice (la alternativa libre a Microsoft Office) permite firmar con certificado digital los documentos OpenDocument creados con sus programas.

Las aplicaciones de Firma son los programas que permiten firmar un documento electrónico. Las tres aplicaciones para firmar documentos más frecuentes ofrecidas por la Administración Pública son:

- **FirmaFacil** ⇒ [9] es una aplicación de firma realizada por el Ministerio de Hacienda y Administraciones Públicas. Su principal objetivo es ofrecer al usuario un sistema

de firma en el que éste pueda firmar cualquier tipo de documento de manera sencilla. El usuario indica qué fichero quiere firmar y la aplicación escoge automáticamente el formato de firma qué debe aplicar, liberando así, al usuario de cualquier duda técnica.

- **Firma** ⇒ [10] La aplicación Firma, realizada por el Ministerio de Hacienda y Administraciones Públicas, es una aplicación java instalable en cualquier sistema operativo. El Cliente Firma es una aplicación avanzada de firma que soporta la firma en múltiples formatos y permite la firma múltiple mediante la co-firma y la contra-firma. Para mayor flexibilidad, Firma permite al usuario elegir el formato en el que desea firmar.
- **eCoFirma** ⇒ [8] realizada por el Ministerio de Industria, es una aplicación de firma que permite generar y validar firmas electrónicas en formato XML XAdES.

Estas aplicaciones, tras descargarlas y ejecutarlas en el ordenador, permiten firmar un documento offline. De esta manera podrás firmar, co-firmar y contra-firmar, además de realizar acciones como cifrado y descifrado de documentos, sin necesidad de estar conectado a la red.

También tenemos una versión Online que es:

- **Valide** ⇒ [20] que es un servicio online de verificación y generación de firmas electrónicas. Proporciona un demostrador de la plataforma firma para facilitar la integración de sus servicios, que pueden realizarse con todos los certificados electrónicos cualificados publicados por cualquier proveedor de servicio de certificación acreditado en España incluido el DNI-e.

2.4.5. Aspectos Legales

Marco regulatorio general de la firma electrónica: [28]

- Directiva 1999/93/CE, de 13 de diciembre, por la que se establece un marco comunitario para la Firma Electrónica.
- Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio-e.
- Ley 59/2003 de 19 de diciembre de Firma Electrónica.
- Real Decreto 1553/2005, de 23 de Diciembre por el que se regula el DNI-e y sus certificados de firma.
- Ley 11/2007 de 22 de Junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP)
- Real Decreto 1671/2009, de 6 de Noviembre, por la que se desarrolla parcialmente la Ley 11/2007.
- Real Decreto 3/2010, de 8 de enero por el que se regula el Esquema Nacional de Seguridad (y RD 4/2010 del Esquena Nacional de Interoperabilidad) en la Administración Electrónica.

- Ley Orgánica 15/1999, de 13 diciembre de Protección de datos de Carácter personal. Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.

LEY DE FIRMA ELECTRÓNICA

La Ley 59/2003, de Firma Electrónica incorpora al derecho español la normativa legal europea en materia de firma electrónica, concretamente la Directiva 1999/93/CE por la que se establece un marco comunitario para la firma electrónica.

La ley regula fundamentalmente las siguientes cuestiones: [28]

- el concepto de firma electrónica.
- los certificados electrónicos.
- los prestadores de servicios de certificación (es decir, que actúan como autoridades de certificación, autoridades de registro, etc.)
- los dispositivos de creación de firma y de verificación de firma.
- el régimen de supervisión y control
- el régimen de infracciones y sanciones.

FIRMA ELECTRÓNICA AVANZADA(Ley 59/2003):

- permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados.
- que está vinculada al firmante de manera única y a los datos a que se refiere.
- y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. [28]

FIRMA ELECTRÓNICA RECONICIDA(Ley 59/2003):

- Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
- Tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel.

Figura 2.9: Firma Electrónica

2.4.6. Requisitos Técnicos

Como requisitos técnicos básicos se debe cumplir:

- La correcta identificación y autenticación de los participantes en los actos administrativos, tanto ciudadanos como Administración.
- La integridad, autenticidad y no repudio de los documentos que forman parte de los expedientes administrativos y la confidencialidad de sus contenidos cuando son transmitidos a través de redes públicas como lo es Internet.
- La disponibilidad de estos documentos para poder acceder a ellos y recuperarlos en cualquier momento.
- La adecuada conservación a estos documentos que se traduce básicamente en que los sistemas dispongan de los mecanismos técnicos que eviten que los documentos no se dañen o extravíen. Se podría añadir además la conservación a largo plazo (el archivado) que implica, entre otras cuestiones, la correcta gestión de las evidencias electrónicas necesarias para probar la autenticidad de los actos administrativos y documentos aportados por los ciudadanos a lo largo del tiempo.

Capítulo 3

Análisis del Sistema

En este capítulo analizamos el problema que queremos resolver, es decir, la implementación de una gestión de certificados mediante una PKI creada por nosotros para mostrar de una manera didáctica el funcionamiento de todas sus componentes y la relación entre ellas.

Empezaremos en el punto 3.1 con el planteamiento del problema. Seguiremos en el punto 3.2 con la perspectiva de la solución. A continuación en el apartado 3.3 mostramos la arquitectura preliminar, describiendo la arquitectura de las PKI y la arquitectura propuesta. Continuamos en el punto 3.4 con la descripción del entorno tecnológico utilizado para la implementación de la solución. También tenemos en este capítulo en el punto 3.5 los diagramas de caso de y uso. Finalmente en el punto 3.6 mostramos el catálogo de requisitos de software.

3.1. Planteamiento del problema

Una vez situados en el contexto en el que se va a desarrollar el proyecto nos ponemos manos a la obra para empezar analizar lo que vamos a hacer. En primer lugar teníamos dos escenarios posibles sobre los cuales la solución podía desarrollarse. Uno era una empresa genérica que quería otorgar una seguridad adicional a sus documentos confidenciales, previamente generados, mediante el uso de certificados digitales para cifrar dichos documentos.

El segundo escenario sería el de la manipulación de datos de pacientes de hospitales, clínicas..., que añaden un plus de confidencialidad a los datos del escenario primero. Además, este segundo escenario incluye complejidades adicionales a la hora de necesitar requisitos de seguridad mayores y una arquitectura más compleja y que se escapan de lo esencial de este proyecto. Que es conocer de una forma didáctica el funcionamiento interno de una PKI y su gestión de certificados y poder aplicarlo a un caso genérico de empresa.

Habiendo aclarado el primer punto, intentamos definir con más claridad lo que queremos hacer para después explicar cómo lo haremos. Lo que queremos es crear nuestra pequeña PKI con los componentes básicos para su correcto funcionamiento y poder tener nuestro propio gestor de certificados digitales. Estos certificados digitales se crearan para los empleados de una empresa genérica. En adelante la palabra empleado y usuario serán sinónimos para indicar que se trata de un empleado de la empresa o lo que es lo mismo un usuario del sistema.

3.2. Perspectiva general de la solución

En nuestro sistema además de los empleados tendremos también tres usuarios especiales que simularan los componentes fundamentales de la PKI , que son la AC (Autoridad de certificación) que es el núcleo de nuestra PKI y la que se encarga de la creación de certificados, revocación de los mismos, así como crear las listas de revocación (CRL) y también de cifrar y firmar los documentos confidenciales para que solo el empleado al que va dirigido pueda verlo. También tendremos otro usuario que será la AR (Autoridad de Registro) que será la encargada de actuar como puente entre los empleados y la AC. Será la encargada de gestionar las solicitudes de certificados de los empleados y una vez analizada y revisado que cumplan todos los requisitos pasárselo a la Ac para que proceda a la creación del certificado. La misma gestión hará para cuando un empleado quiera revocar su certificado, tramitando dicha solicitud y enviándosela a la AC. La AR también será la encargada de gestionar los empleados de nuestro sistema, realizando las altas, bajas y modificaciones correspondientes. Por lo que podemos ver el ciclo de vida de un certificado desde este usuario.

Y el último usuario "especial" es el AV (Autoridad de Verificación), que simulará el elemento de la PKI encargada de comprobar si un certificado se encuentra revocado o no. Algo muy importante a la hora de confiar en un empleado (aunque en este contexto no es tan crítico como podría ser en un entorno más grande o incluso en certificados cuya AC final tiene varios niveles). Si un certificado esta revocado significa que no podríamos utilizar su clave pública para cifrar ya que la relación de confianza entre el titular del certificado y dicha clave ha sido destruida y no tendríamos las garantías de seguridad que nos otorga un certificado que no está revocado. En una implementación profesional las CRL son unas listas que se pueden consultar online (OCSP, Online Certification Status Protocol) o bien descargarse una lista firmada por la propia CA de los certificados revocados. Nosotros hemos optado por implementar dicha CRL mediante tablas en nuestro Sistema Gestor de Base de Datos en Mysql. De ahí que la AV dispondrá de un formulario donde podremos consultar la CRL que queramos o bien buscar si un certificado concreto se encuentra revocado o no.

Habiendo definido los elementos principales del nuestra PKI , ahora nos queda decir qué es lo que aporta esta PKI a nuestros empleados de una determinada empresa. Pues bien, esta empresa tiene una serie de documentos confidenciales que quiere que solo sean "visibles" para la empresa a la cual van dirigidos. Es decir, partimos de que tenemos un documento pdf con datos confidenciales que lo queremos colocar en una localización pública donde tengan acceso todos los empleados de la empresa, pero que sólo lo pueda consultar el titular autorizado. Pues bien, ahí es donde nuestra PKI entra en juego. La AC cogería ese documento y lo cifraría con la clave pública del empleado al que va dirigido y a continuación dicho documento lo firmaría con la clave privada de la AC, para otorgar al documento la garantía de que dicho documento no ha sido modificado una vez creado y que su emisor es quien dice ser.

Esta clave privada de la AC sólo es accesible para el usuario AC y esta guardada en un lugar seguro. Eso es en nuestra aplicación un path que se puede parametrizar en un fichero .ini de la aplicación, pero que una PKI "real" debería estar almacenada en un repositorio público de certificados (generalmente un directorio LDAP) o un lugar con acceso restringido y muy crítico. Para entender el funcionamiento de nuestro sistema es algo secundario, pero que si hay que tenerlo en cuenta debido a la necesidad de custodiar dicho certificado.

Hemos dicho que la AC necesita los certificados que contienen la clave pública de los empleados para poder cifrar dicho documento, por lo que deberán estar en un lugar accesible y público para poder utilizarlos. Esto también será una ruta parametrizable en el fichero .ini de la aplicación al igual que en caso de la clave privada anterior, pero mucho menos crítico. Pero además, como hemos dicho que la AC firma el documento que va a cifrar con la clave pública del empleado, y para firmar dicho documento utiliza la clave privada de la AC, el empleado cuando quiera verificar si dicha firma es correcta, necesitará la clave pública de la AC. Por lo que necesitaremos que este accesible también para todos los usuarios del sistema. Y por tanto también estará parametrizada en el fichero .ini de la aplicación.

Así pues de momento en nuestro análisis necesitamos directorios o carpetas compartidas para depositar en ellas lo siguiente:

- Certificados con la clave pública de los empleados.
- Certificado con la clave pública de la AC.

Vale, pues estas rutas están en el fichero .ini de nuestra aplicación. Pero no hemos dicho nada sobre cómo se crean los certificados digitales. Para esto utilizaremos Makecert, que es una herramienta de creación de certificados X.509 para un uso de desarrollo y que se ejecuta en línea de comando y que viene incluida en Visual Studio, concretamente en el kit de desarrollo (SDK) de Microsoft .Net Framework. Los certificados generados con esta herramienta son con un propósito de prueba y para nuestro desarrollo nos valen perfectamente. Con ella crearemos en primer lugar el certificado de la AC y partir de este certificado generaremos los certificados de todos los empleados.

El certificado de la AC, al ser ella misma la autoridad de certificación, será un certificado autofirmado y en el que van a confiar todos los empleados de la empresa a la hora de realizar los cifrado, descifrado, firma y verificación de esta. Al crear este certificado con **Makecert** tenemos que suministrarle los parámetros que necesitamos para nuestro sistema y adaptarlo a nuestras necesidades. Mediante esta herramienta nos genera dos ficheros, que serán los certificados.

La ejecución de Makecert nos generará dos ficheros. Uno con extensión ".cer"que contiene la clave pública que será empleará para cifrar los documentos y también nos generará otro fichero con extensión ".pvk"que contendrá la clave privada.

Para poder utilizar la clave privada en código y poder descifrar la información cifrada es necesario realizar un paso más que consiste en generar un contenedor de $PKCS\#12$. Para ello tendremos que utilizar otra herramienta ofrecida por Microsoft y que se llama pvk2pfx. Después de ejecutar esto tendremos dos ficheros:

- **Certificado con la clave pública** ⇒ fichero con extensión ".cer" y que será el que compartiremos con todos los empleados para que puedan verificar la firma de la AC.
- **Certificado con la clave privada** ⇒ fichero con extensión ".pfx" y qué será la clave privada de la AC y que se utilizará para cifrar los documentos para los empleados. Debe ser guardado en un lugar seguro y que solo tenga acceso la AC.

Ahora tenemos por tanto los certificados que necesita la AC para poder trabajar. Falta una última cosa que es instalar dichos certificados en el almacén de certificados que ejecutará la maquina donde este la aplicación y en las máquina de los empleados. Lógicamente en las máquinas de los empleados sólo instalaremos el certificado con la clave pública de la AC. Para hacer esto utilizaremos otra herramienta que se llama **"certmgr"**(que viene en el Windows SDK) y que lo que hace es confiar en los certificados creados previamente y que al ser autofirmado tenemos que copiarlo al repositorio raíz de entidades de certificación de confianza (Trusted Root Certification Authorities).

Para llevar un control de todos los empleados, documentos, certificados, revocaciones, listas de revocación (CRL) y demás elementos de nuestro sistema necesitamos almacenarlo en una base de datos. La base de datos que hemos elegido es MYSQL.

Con dicha base de datos, podremos gestionar correctamente el ciclo de vida de un certificado, las solicitudes de certificados y de revocación y todos los datos que queremos recuperar de nuestra PKI . El diseño de la base de datos y sus tablas y relaciones se enseñará en la parte de diseño.

Continuamos, tenemos los certificados de la AC y ahora nos hace falta toda la parte de la aplicación que simulara la PKI y la parte cifrará y firmará los documentos confidenciales de la empresa.

Esta aplicación que hemos desarrollado se basa en las funcionalidades que tiene cada uno de los componentes de la PKI y por tanto hemos optado a que sean estos usuarios "ficticios" los que simularan cada uno de estos componentes.

Empezamos por el componente AR y que será el encargado de realizar la gestión de los empleados del sistema. Aquí tendremos por tanto unos formularios de altas, bajas y modificación para poder gestionar los empleados que utilizaran el sistema. También realizará las labores de gestionar las solicitudes de los empleados que quieran solicitar el certificado digital de la PKI propia. Por tanto se encargará de recibir las solicitudes que realicen los empleados para solicitar dicho certificado, dejando en última instancia la tarea de creación física del certificado a la AC. También se encargará de la gestión de las solicitudes de revocación que soliciten los empleados cuando por ejemplo se haya comprometido su clave privada, perdida o daño en el soporte del certificado, etc. Otra función que tendrá será la de mostrar el ciclo de vida de un certificado de nuestra PKI , desde que se crea hasta que se revoca o expira.

Otro componente sería la AV, cuya función principal sería la consulta de certificados revocados y en que lista se encuentra. Como hemos comentado anteriormente nuestra forma de comprobar si un certificado esta revocado o no, será a través de una consulta a la base de datos por el número de serie del certificado. También deberá permitir consultar los certificados de una CRL concreta y mostrar el estado en que se encuentra un certificado concreto. Es por tanto una función de validación y comprobación de en qué estado se encuentra un certificado que ha generado nuestra PKI .

El otro componente fundamental de la PKI será la AC cuya función principal es la generación de certificados digitales. Esta generación se realiza previa a una solicitud que realiza un empleado a través de la AR y este gestiona y le pasa dicha solicitud, verificada y

aceptada a la AC. Entonces es cuando se crea el certificado digital (que en realidad como hemos explicado se trata de dos ficheros con extensión .cer y .pfx).

Al igual que se encarga de crear los certificados, también se encarga de revocarlos. También previa solicitud del empleado y la aprobación de la AR , aunque también tiene la opción de revocarlos directamente sin que haya una solicitud de revocación previa. También se encarga de gestionar la lista de revocación (CRL) que incluyen los certificados revocados. Estas listas de revocación son las que necesita la AV para realizar las validaciones de certificados. La otra gran tarea que realiza la AC y que es la que mayor utilidad tiene para la empresa es la de cifrar los documentos confidenciales previamente generados. Para cifrarlo necesita la clave privada del empleado al que va dirigido dicho documento. También realiza la firma de dicho documento para garantizar la integridad y autenticidad del mismo. Para firmar utiliza en cambio, la clave privada de la AC que habíamos creado en primer lugar y que es el fichero con la extensión .pfx.

Y nos queda por analizar el usuario empleado que será el que utilizará la PKI y que podrá solicitar la creación de su certificado digital dentro de la PKI . Esta solicitud consistirá en un formulario que se enviará a la AR para que lo tramite y de ésta a la AC. Otra funcionalidad que tendrá la parte de empleados será la de poder solicitar la revocación de un certificado, especificando el motivo por el que se quiere revocar. Esta solicitud pasará también por la AR y de esta otra vez a la AC. También podrá visualizar con el programa Adobe Acrobat (instalado previamente en su equipo) los documentos cifrados por la AC directamente. Y la parte más importante será la de poder cifrar, descifrar, firmar y verificar documentos entre empleados del sistema. Es decir, si el empleado A quiere enviar un documento al empleado B, primero tendrá que cifrarlo con la clave pública del empleado B (certificado con clave pública en nuestro caso) y si quiere adjuntarle la firma de dicho documento tendrá que firmar con la clave privada (certificado con clave privada) del empleado A. El empleado B recibirá el documento cifrado, y para poder descifrarlo tendrá que utilizar la clave privada (certificado con clave privad) del empleado B y poder acceder a su contenido. Si se le envió la firma también tendrá que verificarla utilizando en primer lugar la clave pública del empleado A y por otro el empleado B calcula el hash del documento enviado y lo compara con el que ha descifrado enviado por A.

Esto es en definitiva lo que hace nuestro sistema y como lo hemos querido desarrollar.

3.3. Arquitectura preliminar

Para diseñar la arquitectura preliminar del sistema primero hemos tenido que definir la arquitectura que vaya a tener la PKI que vamos a implementar para luego poder hacer la implementación de la arquitectura que engloba toda la solución.

3.3.1. Arquitecturas PKI

La arquitectura de una PKI describe la organización de sus CAs y sus relaciones de confianza. Cada arquitectura tiene sus ventajas y sus inconvenientes y es apropiada para algunos entornos, mientras que para otros no lo es.

Las opciones que hemos analizado son las siguientes:

- **CA única** ⇒ es la solución más adecuada para comunidades de usuarios pequeña si

se consigue un acuerdo sobre la CA. Los problemas asociados al desarrollo de caminos de certificados y su validación desaparecen. Por contra, el compromiso de la CA es algo catastrófico mientras que su reconstrucción puede ser relativamente sencillo.

- **Certificado con la clave privadListas de confianza simple** ⇒ es la forma más simple de soportar más de una CA. En esta arquitectura hay más de una CA pero no hay relaciones de confianza entre ellas. La principal ventaja de esta arquitectura es su simplicidad. Los caminos de certificados constan de un único certificado y es fácil añadir una nueva CA a la PKI . En cambio, tiene grandes inconvenientes, como que la nueva CA que se desea añadir a la lista debe investigarse previamente. Si se compromete una CA, probablemente se informará rápidamente a sus propios usuarios, pero no a los usuarios de otra CAs ya que la CA comprometida no tiene manera de saber qué usuarios la tienen en su lista.
- **Jerárquica** ⇒ es la mejor solución con una estructura bien definida y se deriva de una forma natural de la propia jerarquía de la organización. La reconstrucción y validación de caminos de certificados son sencillas. Pero puede ser difícil imponer esta estructura a una organización, sobre todo si ya se ha desplegado una colección de CAs independientes. Si una empresa quiere desplegar una PKI jerárquica, es mejor desplegar la CA raíz en primer lugar e integrar en la jerarquía las restantes PKIs a medida que son desplegadas. El compromiso de la CA raíz, es de nuevo, una catástrofe, aunque con las medidas adecuadas de protección es altamente improbable. El compromiso de otra CA es más sencillo de resolver.
- **Malla** ⇒ solución adecuada para organizaciones que no poseen una estructura bien definida. Si previamente se han establecido CAs la PKI en malla es la solución más directa. El compromiso de una CA es catastrófico para sus usuarios, pero las transacciones para los usuarios de las otras CAs no se ven afectadas. La ç complejidad de la construcción y validación de caminos de certificación es un mayor inconveniente.
- **Lista de confianza extendida** ⇒
- **PKIs Cross-certificadas** ⇒ es una estructura sencilla para un reducido número de organizaciones. Sin embargo, deja de ser práctica cuando el número de partes crece o cuando las relaciones entre las organizaciones son dinámicas.
- **Arquitectura de CA puente** ⇒son adecuadas para conectar un gran número de PKIs y también si las relaciones son dinámicas. Las compañías pueden establecer y terminar relaciones rápidamente.

Cabe destacar que ninguna arquitectura es perfecta. Cada una tiene sus ventajas e inconvenientes. La elección depende de los requisitos de la organización.

3.3.2. Arquitecturas propuesta

La arquitectura que vamos a utilizar para implementar la PKI , dentro de las distintas opciones que hay, es la de **CA única**, que para explicar de una forma didáctica el funcionamiento es la más apropiada ya que proporciona todos los certificados y CRL's para una comunidad de usuarios. Todos los usuarios (empleados) confían en la CA que emitió su propio certificado.

Por definición, no pueden añadirse nuevas CAs a la PKI y puesto que sólo hay una única CA no se establecen relaciones de confianza entre otras CA. Los caminos de certificación constan de un único certificado y hay una única CRL . Por el contrario, esta arquitectura

no es escalable y tienen un único fallo, que es que cuando se compromete la CA se invalidan todos los certificados emitidos. Cada usuario deber ser informado inmediatamente. Y Para restablecer la confianza se debe volver a emitir todos los certificados. Y la información sobre el nuevo punto de confianza debe ser distribuida a todos los usuarios. Esta arquitectura sólo es aplicable a una empresa que no necesita comunicarse con el mundo exterior. La figura 3.1 muestra una CA única.

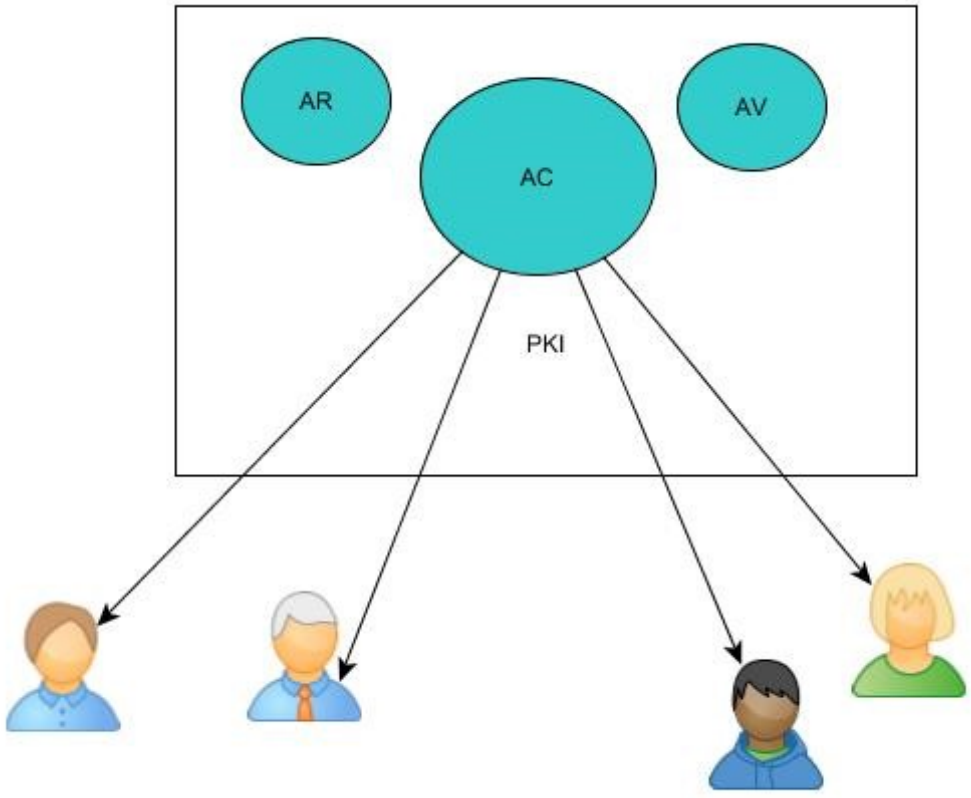


Figura 3.1: CA única

Esta es la idea de la que partimos por tanto para desarrollar nuestra PKI . Si bien, esto hace referencia al número de AC y relaciones de confianza entre los usuarios o empleados, dicha PKI también está compuesta de más elementos que son la AC y AR , entonces en nuestro diseño también lo tenemos que tener en cuenta. Se trataría por tanto de una aplicación que simula el funcionamiento de una PKI , que estaría implementada en .net y con una base de datos de MySql, lo que llevaría a optar por una arquitectura de 3 niveles o capas.

Esta arquitectura posee las siguientes ventajas:

- Si aumenta el tamaño o la complejidad de la base de datos se pueden separar las computadoras.
- No es necesario cambiar la interfaz del usuario si se desea modificar algo en la base de datos y pueden introducirse nuevos clientes sin la necesidad de modificar la base de datos.

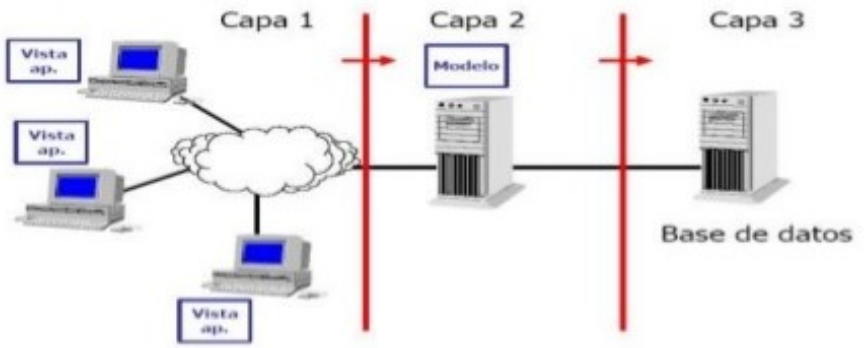


Figura 3.2: Arquitectura de 3 capas.

- El código de cada capa puede ser reutilizado para realizar otras aplicaciones.
- La separación de roles en tres capas, hace más fácil reemplazar o modificar una capa sin afectar a los módulos restantes ya que el código del programa es mucho más entendible.

Pero también presenta inconvenientes:

- Pueden incrementar el tráfico en la red cuando muchos clientes envían peticiones a un solo servidor.
- Requiere más balance de carga.
- Es mucho más difícil programar y probar el software que en arquitectura de dos niveles porque tienen que comunicarse más dispositivos para terminar la transacción de un usuario.

Dónde:

- La capa 1 es la capa de presentación. Donde se incluyen por ejemplo: formularios, informes, respuestas al usuario, etc.
- La capa 2 es la capa de Negocio. Que está formada por las reglas del negocio, validaciones, cálculos, flujos y procesos, etc.
- La capa es la capa de Datos. Formada por base de datos, tablas, procedimientos almacenados, componentes de datos, etc.

En la arquitectura preliminar habíamos integrado en la misma aplicación la parte de empleados y la de la simulación de la PKI . Pensando diferenciar entre una y otra por el rol del usuario que entrara en el sistema y así supuestamente tendríamos una única aplicación Windows que accedería a la base de datos MySql.

3.4. Estudio tecnológico

En este apartado hacemos referencia a las tecnologías utilizadas para la implementación de la solución propuesta y que son por un lado la tecnología .net para el diseño y codificación del modelo de negocio y como base datos hemos optado por MySQL. Como lenguaje de

programación hemos elegido vb.net. El uso de dicha tecnología también nos permite utilizar una herramienta para la generación de certificados de prueba que viene en el SDK de Visual studio y la hemos aprendido su funcionamiento. Dicha herramienta es Makecert, así como otras herramientas relacionadas con los certificados como es pvk2pfx y certutil.

3.4.1. Microsoft.Net

El entorno de desarrollo que hemos utilizado para el proyecto ha sido Microsoft Visual Studio 2010.

El motor de esta tecnología es el Framework que es un entorno de ejecución de aplicaciones informáticas sobre el que se ejecuta cualquier programa desarrollado en .NET en cualquiera de sus lenguajes (VB.NET, Visual C++ .NET, de sus lenguajes (VB.NET, Visual C++ .NET, Visual C# .NET, Visual J#, NetCOBOL, etc.)

Este Framework ofrece un entorno de ejecución común permitiendo una instalación transparente, el fin de las incompatibilidades de DLL y otros componentes, así como las mismas capacidades para todos los lenguajes.Las principales componentes de este entorno son:

- Lenguajes de compilación
- Bibliotecas de clases .Net
- CRL (Common Language Runtime)

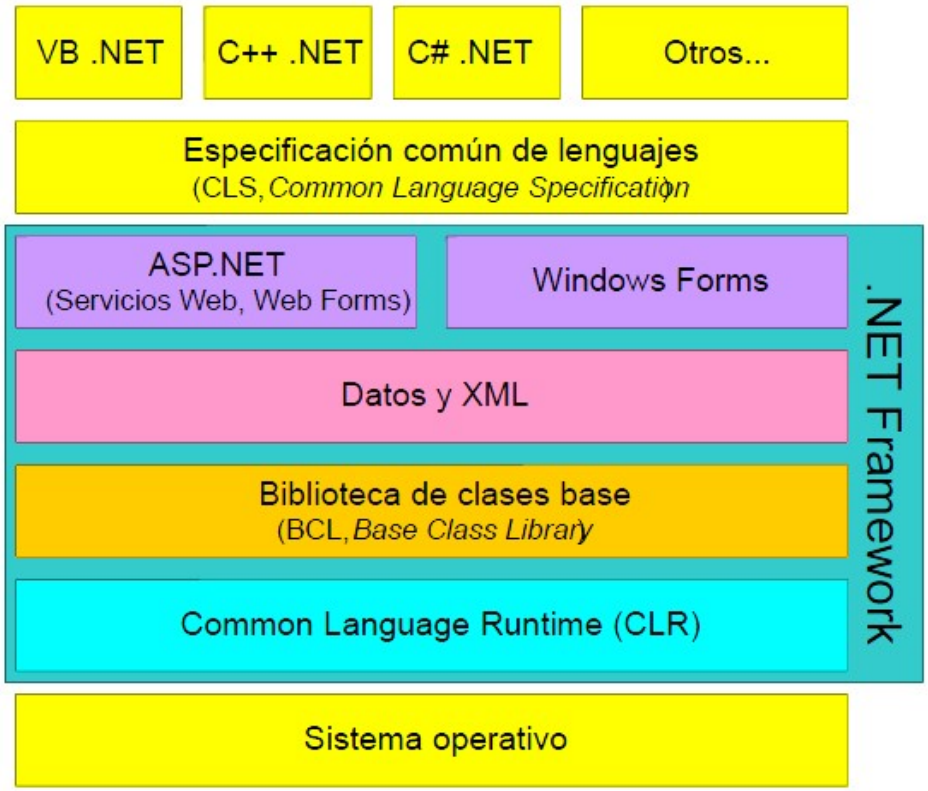


Figura 3.3: Arquitectura de .Net Framework.

Common Language Runtime

El CLR es el verdadero núcleo del framework de .NET, entorno de ejecución en el que se cargan las aplicaciones desarrolladas en los distintos lenguajes, ampliando el conjunto de servicios del sistema operativo. [2]

Permite la integración de distintos lenguajes soportados por la plataforma .Net como como C++, Visual Basic, C#.

La herramienta de desarrollo compila el código fuente de cualquiera de los lenguajes soportados por .NET en un código intermedio, el CIL (Common Intermediate Language) antes conocido como MSIL (Microsoft Intermediate Language), similar al BYTECODE de Java. Para generarlo, el compilador se basa en la especificación CLS (Common Language Specification) que determina las reglas necesarias para crear el código MSIL compatible con el CLR.

Para ejecutarse se necesita un segundo paso, un compilador JIT (Just-In-Time) es el que genera el código máquina real que se ejecuta en la plataforma del cliente. De esta forma se consigue con .NET independencia de la plataforma de hardware. La compilación JIT la realiza el CLR a medida que el programa invoca métodos. El código ejecutable obtenido se almacena en la memoria caché del ordenador, siendo recompilado de nuevo sólo en el caso de producirse algún cambio en el código fuente.

Figura 3.4: Estructura interna del CLR.

Biblioteca de Clases

La Biblioteca de Clases Base (BCL por sus siglas en inglés) maneja la mayoría de las operaciones básicas que se encuentran involucradas en el desarrollo de aplicaciones, incluyendo entre otras (utilizadas para el proyecto):

- Manejo de datos (ADO.NET).
- Cifrado de datos.
- Manejo y administración de excepciones
- Herramientas de seguridad e integración con la seguridad del sistema operativo.
- Manejo de tipo de datos unificado.
- Manipulación de fechas, zonas horarias y periodos de tiempo.
- Manejo de arreglo de datos y colecciones.
- Interacción con el API Win32 o Windows API.
- Compilación de código.

Esta funcionalidad se encuentra organizada por medio de espacios de nombres jerárquicos. La Biblioteca de Clases Base se clasifica, en cuatro grupos clave:

- ASP.NET y Servicios Web XML.
- Windows Forms
- ADO.NET
- .NET

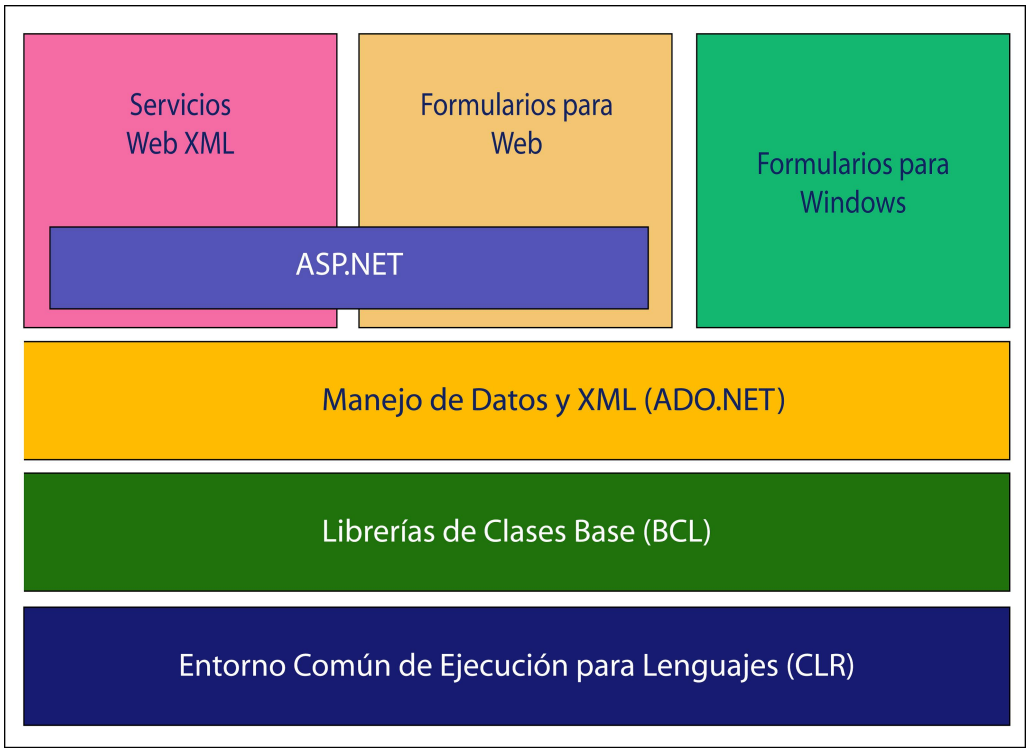


Figura 3.5: Diagrama de la biblioteca de clases

3.4.2. MySql

MySQL es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de doce millones de instalaciones*. [$*$] $\Longrightarrow$ seminario proporcionado en la página de MySQL (año 2009)

Es una de las bases de datos con código abierto más populares del mundo, con las consiguientes ventajas de todo código abierto. Además posee el respaldo de una gran empresa como Sun MicroSysten que después la compró Oracle Corporation.

MySQL es un sistema de administración de bases de datos relacional (RDBMS). También dispone de una herramienta para crear bases de datos de una forma más visual e intuitiva que se llama Workbench. MySQL utiliza el lenguaje de consulta estructurado (SQL).

Las principales características de MySQL son:

- Escrito en C y en C++.
- Probado con un amplio rango de compiladores diferentes.
- Funciona en diferentes plataformas.
- Existen varias APIs que permiten, a aplicaciones escritas en diversos lenguajes de programación, acceder a las bases de datos MySQL.
- Proporciona sistemas de almacenamiento transaccional y no transaccional.
- Utilización de tablas temporales.
- Registros de longitud fija y longitud variable.

3.4.3. Micrsoft Visual Studio

Visual Studio es un conjunto completo de herramientas de desarrollo para la generación de aplicaciones web ASP.NET, Servicios Web XML, aplicaciones de escritorio y aplicaciones móviles. Visual Basic, Visual C# y Visual C++ utilizan todos el mismo entorno de desarrollo integrado (IDE), que habilita el uso compartido de herramientas y hace más sencilla la creación de soluciones en varios lenguajes. Asimismo, dichos lenguajes utilizan las funciones de .NET Framework, las cuales ofrecen acceso a tecnologías clave para simplificar el desarrollo de aplicaciones web ASP y Servicios Web XML.

Permite la creación de soluciones en varios lenguajes y asegura código de calidad durante todo el ciclo de vida de la aplicación, desde el diseño hasta la implementación, facilitando en gran medida la creación de programas y reduciendo el tiempo empleado.

3.4.4. Visual Basic.Net

Visual Basic .NET es un lenguaje de programación de alto nivel de .NET Framework. Cuyas características principales son:

- Diseñador de Windows Forms
- Herramientas para Aplicaciones Windows Forms

- Herramientas para Web Forms
- Herramientas para servicios Web XML
- Soporte de múltiples lenguajes
- Acceso a datos
- Gestión de errores
- Asistentes
- lenguaje orientado a objetos y eventos que soporta encapsulación, herencia y polimorfismo
- Soporte para LINQ

3.5. Diagrama de Casos de uso

En esta sección se muestran los distintos actores que interactúan con el sistema. Para analizar más en detalle los mismos se realiza una descripción gráfica de estos y a continuación una descripción textual de cada uno de ellos. Para la descripción textual utilizaremos la siguiente tabla:

Tabla 3.1: Plantilla para los Casos de Uso

Versión	
ID	
Título	
Actor	□ **Empleado** □ **AC** □ **AR** □ **AV**
Objetivo	
Pre-condición	
Escenario	
Escenario Alternativo	
Post-condición	

Dónde:

- Versión: indica la versión del caso de uso a realizar, en nuestro caso será la 1.0
- Id: (identificador) que es una cadena de caracteres que identifica de manera unívoca cada caso de uso. La nomenclatura tendrá el siguiente patrón "CU-XX", donde XX se sustituirá por un número ordinal de forma creciente.
- Título: Breve descripción del objetivo del caso de uso. Debe mostrar el propósito del mismo con un simple vistazo.
- Actor: Agente externo que interactúa con el sistema.

- Objetivo: Explicación textual del caso de uso.
- Pre-condición: son las condiciones que se deben cumplir previamente para poder realizar el caso de uso.
- Escenario: Ejecución detallada del caso de uso.
- Escenario alternativo: Ejecución alternativa del caso de uso.
- Post-condición: Estado que presenta el sistema tras la ejecución de una determinada operación

3.5.1. Definición de actores

En nuestro sistema existen cuatro tipos de actores que pueden interactuar con el sistema y que son:

- Empleados: usuario o empleado de la empresa que accede a la aplicación cliente de GesCert
- AC: usuario que simula el funcionamiento de la Autoridad de Certificación.
- AR: usuario que simula el funcionamiento de la Autoridad de Registro.
- AV: usuario que simula el funcionamiento de la Autoridad de Verificación.

3.5.2. Diagrama de Caso de uso para Empleados

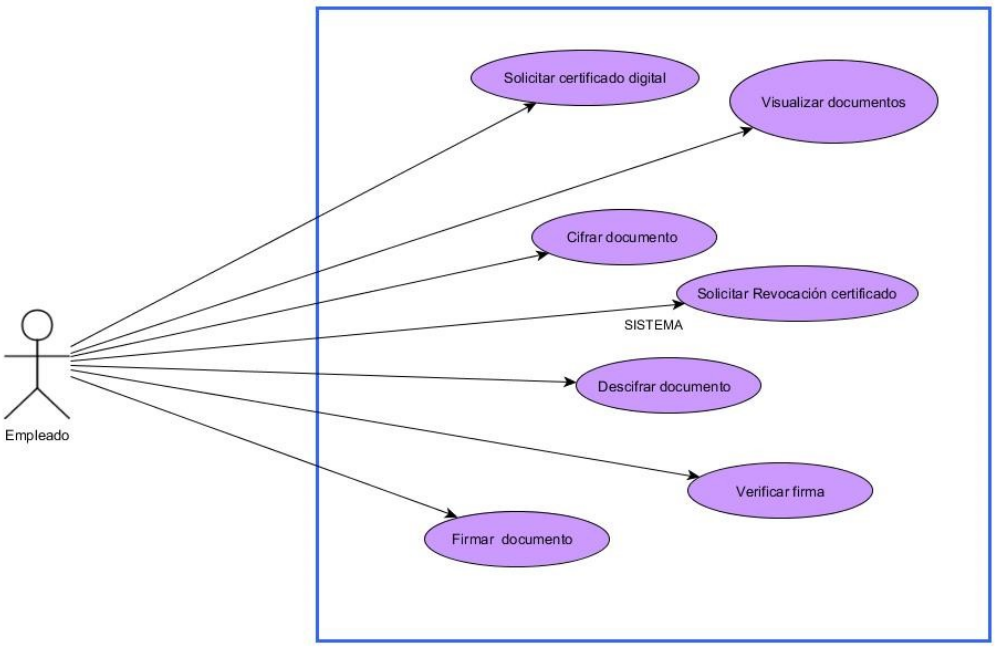


Figura 3.6: Caso de uso de empleado.

Este actor es el encargado de interactuar con la PKI y representa a cualquier empleado de la empresa que utiliza la PKI para solicitar la creación de un certificado, enviándoselo a la AR. Además también puede interactuar con la PKI solicitando la revocación de su certificado (habiendo realizado antes la solicitud) cuando por algún motivo dicho certificado tiene que dejar de estar operativo, como por ejemplo cuando se ha comprometido su clave

privada, ha dejado de trabajar para la empresa, etc.

El empleado puede además visualizar con el programa Adobe Acrobat la visualización de documentos que están cifrados y que ha AC ha cifrado y firmado para él sin necesidad de descifrarlos previamente, el propio visualizar se encarga de descifrarlo y mostrar el contenido de dicho pdf.

Y por último, los empleados pueden intercambiarse información entre ellos utilizando las certificados con claves pública que están en una ubicación con acceso público, cifrando los documentos que se quieren enviar y firmándolos. El receptor descifrará el mensaje y verificará la firma. Para hacer esto no necesitan interactuar con la PKI ya que es la aplicación cliente que cada empleado tiene en su equipo la encargada de realizar estas acciones. Ver Figura 3.6.

Tabla 3.2: Caso de Uso UC-01. Solicitud de certificado digital

Versión	**1.0**
ID	**UC-01**
Título	**Solicitud de certificado digital**
Actor	☒ **Empleado** ☐ **AC** ☐ **AR** ☐ **AV**
Objetivo	**Solicitar un certificado Digital a la Autoridad de Registro (AR)**
Pre-condción	▪ Usuario dado de alta en la BD. ▪ La base de datos está levantada. ▪ El usuario mostrará el DNI a la persona que gestiona la solicitud ▪ Que el usuario no tenga ya un certificado digital, ya que solo puede disponer uno en dicha empresa.
Escenario	1. El usuario rellena los campos del formulario. 2. El usuario pulsa el botón de enviar. 3. Se inserta en la tabla "SolicitudCertificado" con estado = Recibido.
Escenario Alternativo	
Post-condición	**Se visualiza por pantalla un mensaje de solicitud enviada. Se inserta el registro en la tabla de "solicitudcertificado".**

Tabla 3.3: Caso de Uso UC-02. Solicitud Revocación certificado

Versión	**1.0**
ID	**UC-02**
Título	**Solicitud Revocación certificado**
Actor	☒ **Empleado** ☐ **AC** ☐ **AR** ☐ **AV**
Objetivo	**Solicitar la revocación de un certificado que tiene un usuario por el motivo por el cual quiere solicitar.**
Pre-condción	▪ El usuario debe tener un certificado. ▪ El certificado debe estar emitido. ▪ La base de datos está levantada.
Escenario	1. El usuario/empleado selecciona el certificado del que quiere solicitar su revocación mediante: *a*) Número Serie Certificado. *b*) DNI del empleado. 2. Selecciona el motivo por el cual quiere revocarlo de la lista de opciones posibles. 3. Solicita la revocación a la AR . 4. Se muestra el certificado del empleado en un Listview.
Escenario Alternativo	**1-2. El empleado ha introducido un DNI o Número serie incorrecto.** 1. No se muestra el certificado en el Listview 2. Volver al paso 1certificado pasa a estado “Pre-revocado” mientras la AR gestiona la solicitud.
Post-condición	▪ El certificado pasa a estado “Pre-revocado” mientras la AR gestiona la solicitud.

Tabla 3.4: Caso de uso UC-03. Visualizar documentos.

Versión	**1.0**
ID	**UC-03**
Título	**Visualizar dcoumentos.**
Actor	☒ **Empleado** ☐ **AC** ☐ **AR** ☐ **AV**
Objetivo	**El empleado visualizará en Adobe Acrobat los documentos que están cifrados con su clave pública.**
Pre-condción	▪ El documento esta creado y cifrado con la clave pública del empleado que lo quiere visualizar. ▪ La base de datos está levantada.
Escenario	**El empleado selecciona el documento cifrado que quiere visualizar.**
Escenario Alternativo	**El documento a visualizar no está cifrado con la clave pública del empleado y no le permite visualizarlo.**
Post-condición	**El documento se abre con Adobe Acrobat.**

Tabla 3.5: Caso de uso UC-04. Cifrar documento.

Versión	**1.0**
ID	**UC-04**
Título	**Cifrar documento (entre empleados).**
Actor	☒ **Empleado** ☐ **AC** ☐ **AR** ☐ **AV**
Objetivo	**El empleado cifra un documento con la clave pública del empleado al que se lo quiere enviar.**
Pre-condción	▪ El empleado al que le quiere enviar el documento tiene que tener un certificado con clave pública en el repositorio donde están todos los certificados públicos (con extensión .cer). ▪ El documento a enviar no está cifrado. ▪ La base de datos está levantada.
Escenario	1. El empleado selecciona el documento cifrado que quiere visualizar. 2. Se cargan automáticamente los certificados que tiene el empleado en su equipo en un Listview. 3. Seleccionar el certificado buscando el archivo o desde el Listview que se carga en 1. 4. Una vez seleccionado el certificado pulsamos el botón de Cifrar. 5. Se verifica que el certificado seleccionado no este expirado ni revocado.
Escenario Alternativo	**5a. Si el certificado seleccionado se encuentra expirado o revocado no se puede cifrar el documento.** ▪ Vuelve al paso 1.
Post-condición	**El documento seleccionado se cifra con el nombre del fichero igual que el original sustituyendo la extensión pdf por una parametrizable (por defecto .enc) y lo deja en la ruta que viene especificada en el fichero .ini de la aplicación.**

Tabla 3.6: Caso de uso UC-05. Descifrar documento (entre empleados).

Versión	**1.0**
ID	**UC-05**
Título	**Descifrar documento (entre empleados).**
Actor	☒ **Empleado** ☐ **AC** ☐ **AR** ☐ **AV**
Objetivo	**El empleado descifra un documento que le ha enviado otro empleado con su certificado con clave privada (la del receptor).**
Pre-condción	▪ El empleado quiere descifrar un documento que le ha enviado otro empleado. Para ello utiliza su clave privada en el certificado con extensión .pfx. ▪ El documento a descifrar está cifrado. ▪ La base de datos está levantada.
Escenario	1. El empleado selecciona el documento cifrado que ha cifrado el empleado emisor del documento. 2. Se cargan automáticamente los certificados que tiene el empleado en su equipo en un Listview. 3. Seleccionar el certificado buscando el archivo o desde el Listview que se carga en 1. 4. Una vez seleccionado el certificado pulsamos el botón de Descifrar. 5. No hace falta verificar el certificado porque ya lo verifico el emisor del documento.
Escenario Alternativo	**4 a. Si el certificado seleccionado no tiene la clave privada para poder descifrar no se puede continuar.** ▪ Vuelve al paso 3. **4 b. Si el certificado utilizado para descifrar no es del mismo empleado no concuerdan la clave pública y privada y no se podrá descifrar.** ▪ Vuelve al paso 3.
Post-condición	**El documento seleccionado se descifra con el nombre del fichero igual y con extensión .pdf. Y lo deja en la carpeta que viene especificada en el fichero .ini de la aplicación.**

Tabla 3.7: Caso de uso UC-06. Firmar documento.

Versión	**1.0**
ID	**UC-06**
Título	**Firmar documento (entre empleados).**
Actor	☒ **Empleado** ☐ **AC** ☐ **AR** ☐ **AV**
Objetivo	**El empleado firma con su clave privada un documento que va a enviar a otro empleado.**
Pre-condción	▪ El empleado quiere firmar el documento tiene que tener un certificado con su clave privada para poder firmar (certificado con extensión .pfx). ▪ La base de datos está levantada.
Escenario	1. El empleado selecciona el documento que quiere cifrar. 2. El empleado selecciona el certificado que contiene su clave privada (.pfx). 3. El empleado pulsa el botón "Firmar". 4. Una vez seleccionado el certificado pulsamos el botón de Descifrar. 5. No hace falta verificar el certificado porque ya lo verifico el emisor del documento.
Escenario Alternativo	**2 a. Si el certificado seleccionado no tiene la clave privada para poder firmar no se puede continuar.** ▪ Vuelve al paso 1. **4 b. Si el certificado utilizado para descifrar no es del mismo empleado no concuerdan la clave pública y privada y no se podrá descifrar.** ▪ Vuelve al paso 3.
Post-condición	**Se obtiene un documento firmado con la clave privada del firmante, con una extensión que se asigna en el fichero .ini y en una ruta que también viene en dicho fichero. Mensaje que indica si la firma se ha realizado correctamente o no.**

Tabla 3.8: Caso de uso UC-07. Verificar firma documento.

Versión	**1.0**
ID	**UC-07**
Título	**Verificar firma documento (entre empleados).**
Actor	☒ **Empleado** ☐ **AC** ☐ **AR** ☐ **AV**
Objetivo	**El empleado verifica la firma de un documento que le ha enviado otro empleado previamente.**
Pre-condción	▪ El empleado que quiere verificar la firma necesita la clave pública del empleado emisor del mensaje (certificado con extensión .cer). ▪ El empleado que verifica la firma necesita el documento original, que previamente ha descifrado en la opción de descifrar documento. ▪ La base de datos está levantada.
Escenario	1. El empleado selecciona el documento original que quiere verificar (previamente lo ha descifrado y lo puede ver). 2. El empleado selecciona el documento firmado que le ha enviado el empleado emisor. 3. El empleado selecciona el certificado con la clave pública del empleado emisor del documento (certificado con extensión .cer). 4. Pulsar el botón de "verificar firma".
Escenario Alternativo	**4a. Si el certificado seleccionado no pertenece al empleado emisor se producirá un mensaje de error al intentar verificar la firma del documento.** ▪ Vuelve al paso 3. **4 b. Si el documento firmado no se corresponde con el documento original la verificación de la firma mostrará un mensaje de error.** ▪ Vuelve al paso 1.
Post-condición	**Se verifica si la firma enviada por el empleado emisor coincide con los datos.**

3.5.3. Diagrama de Caso de uso para AV

En este apartado describimos las capacidades del actor AV (Autoridad de verificación), traducido del inglés VA - Verification Authority, ver Figura 3.7.

Este actor es el encargado de simular la componente AV de la PKI y para ello se encarga de mostrar la información que hay en el sistema sobre un certificado concreto. También permite la consulta de las CRL que se han almacenado en la BD y mostrar que certificados revocados pertenecen a dicha CRL, así como permitir la búsqueda de un certificado para saber si esta revocado o no.

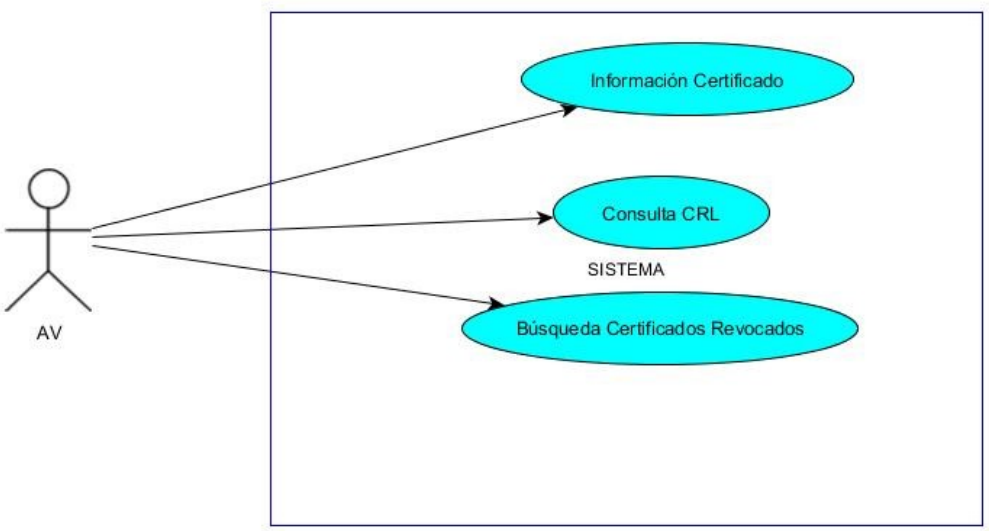


Figura 3.7: Caso de uso para AV.

Tabla 3.9: Caso de uso UC-08. Información Certificado.

Versión	**1.0**
Título	**UC-08**
Título	**Información Certificado.**
Actor	☐ **Empleado** ☐ **AC** ☐ **AR** ☒ **AV**
Objetivo	**Consulta el estado en que se encuentra un certificado emitido por la PKI.**
Pre-condción	▪ El certificado a consultar debe estar creado previamente o al menos realizado por parte del empleado de una solicitud de creación del mismo. ▪ La base de datos está levantada.
Escenario	**La AV introduce el número de serie del certificado que quiere consulta y pulsa el botón de "buscar certificado".**
Escenario Alternativo	**Si el número de serie introducido es incorrecto o no existe.**
Post-condición	**Muestra los datos del certificado a buscar.**

Tabla 3.10: Caso de uso UC-09. Consulta de CRL.

Versión	**1.0**
ID	**UC-09**
Título	**Consulta de CRL.**
Actor	☐ **Empleado** ☐ **AC** ☐ **AR** ☒ **AV**
Objetivo	**Muestra todas las listas de CRL que ha tenido, así como la actual de una PKI así como los certificados revocados que contiene dicha lista.**
Pre-condción	▪ Que haya al menos una CRL en la PKI. ▪ La base de datos está levantada.
Escenario	1. Se muestra un formulario de búsqueda de CRL y certificados revocados para buscarlos por número de CRL o por fecha, tanto de emisión de la CRL como de revocación. También permite la búsqueda directa por el número de la CRL. 2. Se muestran en un Listview las CRL que cumplen con los requisitos de búsqueda de (1). 3. Seleccionar un elemento del Listview de CRL y pulsar el botón de "Seleccionar CRL" para buscar los certificados revocados que tiene dicha CRL. 4. Si tiene certificados revocados esa CRL aparecerán en el Listview de certificados revocados. Si marcamos uno y pulsamos el botón "Detalle certificado" nos muestra un nuevo formulario emergente con los datos del certificado marcado.
Escenario Alternativo	
Post-condición	**Muestra en los Listview la CRL , certificados revocados de dicha CRL e información del certificado revocado seleccionado.**

Tabla 3.11: Caso de uso UC-10. Búsqueda de certificados revocados.

Versión	**1.0**
ID	**UC-10**
Título	**Búsqueda de certificados revocados.**
Actor	☐ **Empleado** ☐ **AC** ☐ **AR** ☒ **AV**
Objetivo	**Búsqueda de certificados revocador por la PKI tanto de la CRL actual como de anteriores CRL . Permite realizar la búsqueda por fecha de revocación del certificado, por motivo de revocación o por número de serie del certificado.**
Pre-condción	▪ La base de datos está levantada. ▪ El certificado fue revocado.
Escenario	Formulario para realizar la búsqueda de certificados revocados según los criterios de búsqueda de fecha de revocación, número de serie del certificado o motivo de revocación.
Escenario Alternativo	
Post-condición	**El /los certificados que cumplen las condiciones de búsqueda se muestran en un Listview.**

3.5.4. Diagrama de Caso de uso para AR

En este apartado describimos las capacidades del actor AR (Autoridad de Registro), traducido del inglés RA - Registration Authority, ver Figura 3.8.

Este actor es el encargado de simular la componente AR de la PKI y el encargado fundamentalmente de realizar las gestiones de solicitudes de certificados y de revocación de certificados entre los empleados y la PKI. Tendría que verificar que la información transmitida por los empleados para la creación del certificado es correcta y está completa.

Otra función importante es que se encarga de la gestión de los empleados en el sistema, realizando el alta, baja, modificación, así como la consulta de cualquier empleado. Además permite mostrar el ciclo de vida de cualquier certificado del sistema.

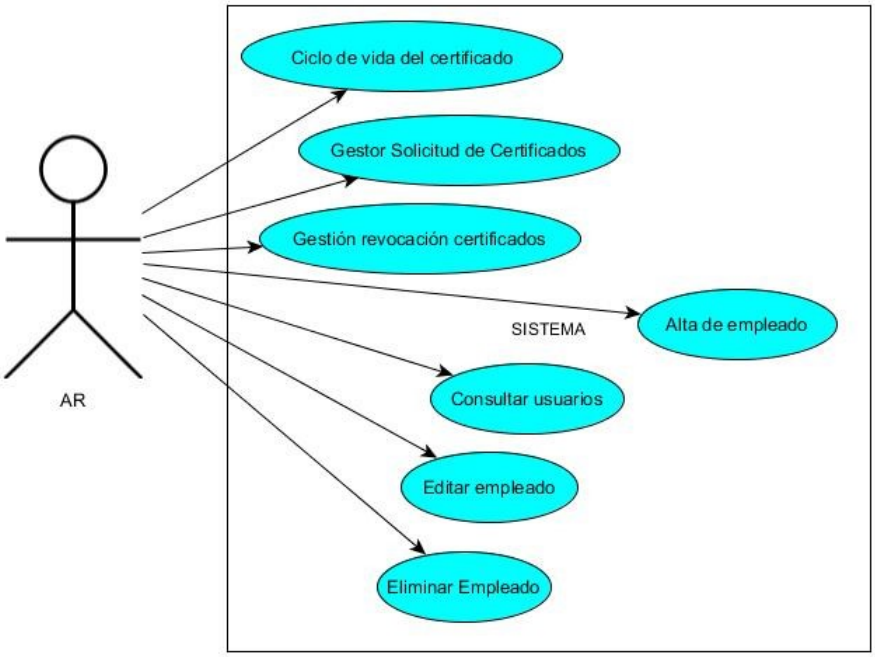


Figura 3.8: Caso de uso para AR .

Tabla 3.12: Caso de uso UC-11. Ciclo de vida del Certificado.

Versión	**1.0**
ID	**UC-11**
Título	**Ciclo de vida del certificado**
Actor	☒ **Empleado** ☐ **AC** ☐ **AR** ☐ **AV**
Objetivo	**Muestra en un formulario el ciclo de vida de un certificado emitido por la PKI desde que se crea hasta que expira o se revoca.**
Pre-condción	▪ La base de datos está levantada. ▪ El certificado a buscar debe existir.
Escenario	1. Se introduce el número de serie del certificado a buscar o el DNI del titular del certificado 2. Se cargan en el formulario todos los datos relativos a dicho certificado que tenemos en la Base de datos. Desde que se solicita, los estados por los que ha pasado y si ha sido revocado o no.
Escenario Alternativo	
Post-condición	**Datos cargados en el formulario de dicho certificado.**

Tabla 3.13: Caso de uso UC-12. Gestor Solicitud de Certificados.

Versión	**1.0**
ID	**UC-12**
Título	**Gestor Solicitud de Certificados.**
Actor	☐ **Empleado** ☐ **AC** ☒ **AR** ☐ **AV**
Objetivo	**Formulario que simula una AR cuando recibe las solicitudes de certificados de los empleados y las acciones que toma sobre dichas solicitudes, que son tramitarlas, aceptar la solicitud y pasárselo a la AC para que cree el certificado o denegar dicha solicitud.**
Pre-condción	▪ La base de datos está levantada. ▪ Existen solicitudes de certificados de los empleados.
Escenario	1. En primer lugar la AR realiza la búsqueda de las solicitudes enviadas por los empleados para solicitar un certificado digital de la PKI . Esta búsqueda se puede realizar filtrando por el estado de la solicitud de los certificados que puede ser: "recibido" ⇒ que es el estado en el que esta una solicitud de un empleado nada más enviarse, sin que la AR haya realizado ninguna acción sobre dicha solicitud. "En trámite" ⇒ cuando la AR está analizando la solicitud para ver si cumple los requisitos y demás condiciones. 2. Acción a realizar sobre los certificados seleccionados: *a*) Tramitar Seleccionados ⇒ sirve para cambiar el estado de la solicitud de certificado simulando que la AR está analizando dicha solicitud enviada. *b*) Aceptar seleccionados ⇒ con ella indicamos que una AR ha aceptado la solicitud del certificado y dicha solicitud se traslada a la AC para que proceda a la creación del certificado. Esta acción lleva además la creación de un registro de certificado en estado "Preactivado" hasta que lo cree físicamente la AC. *c*) Denegar Seleccionados ⇒ mediante la cual simulamos la denegación de la AR a una solicitud de certificado.
Escenario Alternativo	
Post-condición	**Solicitudes de certificados de empleados gestionadas por la parte que simula la AR del sistema.**

Tabla 3.14: Caso de uso UC-13. Gestión revocación certificados.

Versión	**1.0**
ID	**UC-13**
Título	**Gestor revocación de certificados**
Actor	☐ **Empleado** ☐ **AC** ☒ **AR** ☐ **AV**
Objetivo	**Formulario que simula una AR cuando recibe las solicitudes de revocación de certificados de los empleados y las acciones que toma sobre dichas solicitudes, que son tramitarlas y aceptar la solicitud y pasárselo a la AC para que revoque el certificado del empleado.**
Pre-condción	▪ La base de datos está levantada. ▪ El empleado ha realizado una solicitud de revocación de certificado.
Escenario	1. Se buscan las solicitudes de revocación de certificados realizados por los empleados, bien mostrando todas la que hay o filtrando por el estado en que se encuentran y que son "recibidas" ⇒ cuando el empleado solicita la revocación y "En trámite" ⇒ cuando la AR está analizando dicha solicitud. 2. De las solicitudes seleccionadas la AR simula una de las siguientes acciones: *a*) "Tramitar Seleccionados" ⇒ consiste en cambiar de estado las solicitudes recibidas por el cliente y que no han sido analizadas aun. El estado en que se queda dicha solicitud es "En Tramite". *b*) "Aceptar Seleccionados" ⇒ consiste en simular que la Ar acepta la solicitud que estaba en estado de tramite o directamente la que acaba de llegarla en la solicitud. Este estado indica que se pasa a la AC para que proceda a realizar la revocación del certificado, añadiéndolo a al CRL que está en vigor.
Escenario Alternativo	
Post-condición	**Mensaje por pantalla indicando la tarea realizada.**

Tabla 3.15: Caso de uso UC-14. Alta de empleados.

Versión	**1.0**
ID	**UC-14**
Título	**Alta de empleados.**
Actor	☐ **Empleado** ☐ **AC** ☒ **AR** ☐ **AV**
Objetivo	**Dar de alta a un empleado en el sistema.**
Pre-condción	▪ La base de datos está levantada. ▪ El empleado no está dado de alta en el sistema.
Escenario	1. La AR muestra el formulario de alta del empleado. 2. La AR introduce los datos en el sistema. 3. El sistema valida que el DNI del usuario no está en el sistema. 4. El sistema valida que no hay datos obligatorios vacíos y que el formato sea correcto. 5. El sistema crea un nuevo empleado.
Escenario Alternativo	
Post-condición	▪ Se da de alta al nuevo usuario en el sistema. ▪ Se muestra por pantalla un mensaje confirmando el alta del usuario..

Tabla 3.16: Caso de uso UC-15. Consultar usuarios.

Versión	**1.0**
ID	**UC-15**
Título	**Consultar usuarios.**
Actor	☐ **Empleado** ☐ **AC** ☒ **AR** ☐ **AV**
Objetivo	**Visualizar los empleados del sistema.**
Pre-condción	▪ La base de datos está levantada.
Escenario	1. La Ar selecciona la opción de gestionar empleados 2. El sistema recupera la lista de los empleados.
Escenario Alternativo	
Post-condición	**Se visualizan los empleados dados de alta en el sistema.**

Tabla 3.17: Caso de uso UC-16. Editar empleado.

Versión	**1.0**
ID	**UC-16**
Título	**Editar empleado.**
Actor	☐ **Empleado** ☐ **AC** ☒ **AR** ☐ **AV**
Objetivo	**Editar la información de un empleado.**
Pre-condción	▪ La base de datos está levantada.
Escenario	1. La AR selecciona la opción de gestionar empleados. 2. La AR selecciona la opción de editar. 3. El sistema muestra el formulario con la información del empleado. 4. La AR actualiza la información del empleado. 5. El sistema valida que no hay datos obligatorios vacíos y que el formato de datos es correcto. El sistema actualiza los datos del empleado modificado.
Escenario Alternativo	**6 b. Dato obligatorio vacío o error de formato.**
Post-condición	1. Se actualiza en el sistema la información del empleado. 2. Se muestra por pantalla un mensaje de la actualización del empleado.

Tabla 3.18: Caso de uso UC-17. Eliminar empleado.

Versión	**1.0**
ID	**UC-17**
Título	**Eliminar Empleado.**
Actor	☐ **Empleado** ☐ **AC** ☒ **AR** ☐ **AV**
Objetivo	**Dar de baja a un empleado del sistema.**
Pre-condción	▪ La base de datos está levantada. ▪ El empleado esta dado de alta en el sistema.
Escenario	1. La AR selecciona la opción de eliminar empleado. 2. La AR selecciona el empleado que quiere eliminar. 3. La AR selecciona la opción de eliminar. 4. Al eliminar un empleado se eliminará el certificado si lo tuviera y demás registros asociado a dicho certificado. 5. La AR confirma la opción de eliminar. 6. El sistema elimina al empleado.
Escenario Alternativo	**5 a. Cancelar la opción de eliminar.**
Post-condición	▪ Se elimina al empleado del sistema. ▪ Se muestra un mensaje indicando la baja del empleado.

3.5.5. Diagrama de Caso de uso para AC

En este apartado describimos las capacidades del actor AC (Autoridad de certificación), traducido del inglés CA - Certification Authority, ver Figura 3.9.

Este actor es el que simula el componente AC de la PKI y es el motor de la PKI. Su principal función es la crear los certificados digitales a los empleados, previa solicitud de los empleados. Una vez creados, los empleados podrán hacer uso de la aplicación cliente que tendrán en sus equipos. También se encarga de revocar los certificados de los empleados, hayan realizado una petición o directamente sin haberla recibido.

Otra función de la AC es la creación de las CRL del PKI, permitiendo crear una nueva y añadir certificados revocados a dicha lista.

Otra de las funciones fundamentales de la AC sobre todo para la empresa que lo implantará es la de cifrar los documentos confidenciales de los empleados que a través de la AC se realiza así como la firma de dicho documento para asegurar la integridad y no repudio de los mismos. La última funcionalidad de la AC es la de tener "la última palabra" para la creación y denegación de certificados previo autorización o denegación de la AR.

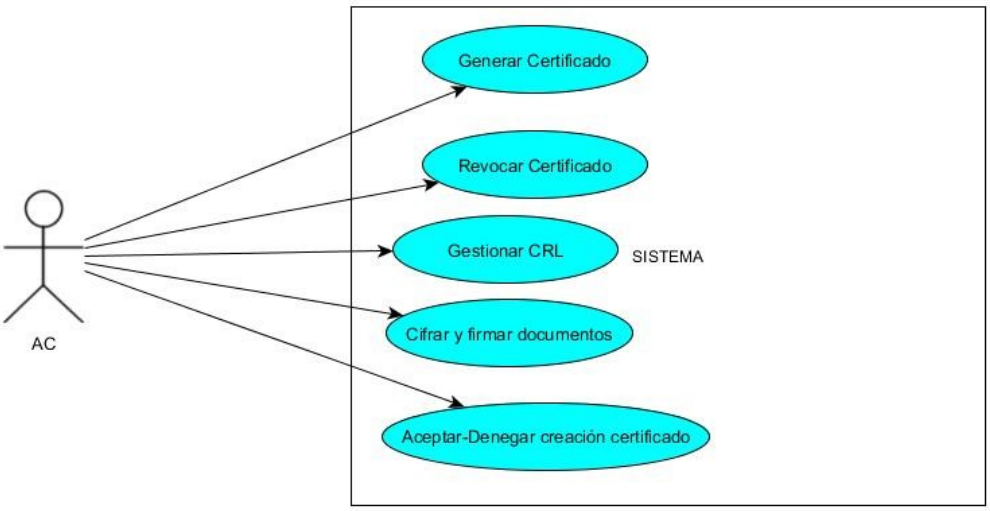


Figura 3.9: Caso de uso para AC.

Tabla 3.19: Caso de uso UC-18. Generar Certificados.

Versión	**1.0**
ID	**UC-18**
Título	**Generar Certificados.**
Actor	☐ **Empleado** ☒ **AC** ☐ **AR** ☐ **AV**
Objetivo	**La AC se encarga de generar físicamente los certificados de un empleado previa solicitud de creación. La AC generará dos ficheros, un certificado con la clave pública del empleado y con extensión .cer y otro con la clave privada y con extensión .pfx. El de la clave pública lo depositará en una carpeta común para todos los empleados y a la que tendrán accesos todos.**
Pre-condción	▪ La base de datos está levantada. ▪ El certificado a crear se encuentra en estado "Pre-Activado".
Escenario	1. La AC selecciona la opción generar certificados 2. La Ac introduce el DNI del empleado que va a generar el certificado. 3. Se cargan los datos del titular del certificado que se crearon al aceptar la solicitud del certificado. 4. La AC rellena el resto de datos referentes a la creación física del certificado. 5. El sistema valida que se hayan introducido los datos obligatorios. 6. Se crean con la herramienta Makecert dos ficheros, uno con la clave pública y extensión .cer y otro con la clave privada con extensión .pfx. 7. El certificado se actualiza a estado "Activado" y está operativo para poder usarse para cifrar, descifrar, firmar y verificar firma.
Escenario Alternativo	**6 a. Parámetros incorrectos para la creación de certificados.**
Post-condición	▪ Certificados con clave pública y clave privada creados correctamente. ▪ Mensaje de confirmación de certificado creado.

Tabla 3.20: Caso de uso UC-19. Revocar Certificado.

Versión	**1.0**
ID	**UC-19**
Título	**Revocar Certificado.**
Actor	☐ **Empleado** ☒ **AC** ☐ **AR** ☐ **AV**
Objetivo	**Revoca un certificado de un empleado del sistema.**
Pre-condción	▪ La base de datos está levantada. ▪ Existen unas solicitudes de revocación por parte de los empleados previamente.
Escenario	1. La AC selecciona la opción de revocar certificado. 2. Selecciona las solicitudes de certificados que están en el sistema. Filtrando por el estado en que se encuentran dichas solicitudes. Estos filtros pueden ser por solicitudes en trámite y solicitudes aceptadas. Si selecciona "todos los certificados" se mostraran todos los certificados del sistema aunque no hayan realizado ninguna solicitud de revocación de certificado. 3. Se muestran los certificados en un Listview que cumplen los criterios de búsqueda de la AC. 4. La AC marcará del Listview los certificados que quiere recovar y selecciona el motivo por los que los quiere revocar. 5. Pulsara el botón de revocar y los certificados y hará lo siguiente el sistema: *a*) Actualizar el estado del certificado a revocar poniéndolo como revocado. *b*) Insertarlo en la lista de certificados revocados de la CRL que está activa en ese momento.
Escenario Alternativo	
Post-condición	▪ Certificados seleccionados del Listview recovados. ▪ Mensaje de confirmación de revocación.

Tabla 3.21: Caso de uso UC-20. Aceptar / Denegar creación certificados.

Versión	**1.0**
ID	**UC-20**
Título	**Aceptar / Denegar creación certificados.**
Actor	☐ **Empleado** ☒ **AC** ☐ **AR** ☐ **AV**
Objetivo	**La AC acepta o deniega las solicitudes de certificados que esta tramitado previamente la AR y están pendientes de aceptar o denegar.**
Pre-condción	▪ La base de datos está levantada. ▪ Las solicitudes de certificados han sido tramitadas previamente por la AR .
Escenario	1. La AC selecciona las solicitudes que están en trámite y aún no han sido aceptada por la AR , es decir las acepta directamente sin esperar a la autorización de la AR. 2. La AC deniega las solicitudes que la AR denegó.
Escenario Alternativo	
Post-condición	**Solicitudes de certificados aceptadas o denegadas correctamente.**

Tabla 3.22: Caso de uso UC-21. Gestionar CRL.

Versión	**1.0**
ID	**UC-21**
Título	**Gestionar CRL.**
Actor	☐ **Empleado** ☒ **AC** ☐ **AR** ☐ **AV**
Objetivo	**Formulario que simula la creación de una nueva CRL en el sistema activa y que permite añadir directamente certificados revocados a la misma sin que se haya creado previamente una solicitud de revocación de certificado.**
Pre-condción	▪ La base de datos está levantada.
Escenario	1. La AC selecciona la opción de Gestionar CRL 2. Se carga en el sistema los datos necesarios para crear una nueva lista CRL. 3. La AC rellena los datos obligatorios necesarios para crear la nueva CRL. 4. El AC pulsa el botón de "Crear CRL" y la nueva AC se creará. 5. Podemos marcar directamente un certificado como revocado sin que haya habido previamente una solicitud de revocación y lo hace la AC. 6. Introducir el número de serie del certificado que queremos revocar, la fecha en la que lo revocamos y el motivo por el que lo revocamos. 7. Pulsamos el botón "Añadir certificado a CRL" y se creará el certificado revocado en la CRL que este activa en el momento.
Escenario Alternativo	**6 a. El número de serie introducido no es correcto. Volver a 6.**
Post-condición	▪ Nueva lista CRL creada ó. ▪ Nuevo certificado revocado. ▪ Mensaje indicando una u otra opción.

Tabla 3.23: Caso de uso UC-22. Cifrar y firmar documentos.

Versión	**1.0**
ID	**UC-22**
Título	**Cifrar y firmar documentos.**
Actor	☐ **Empleado** ☒ **AC** ☐ **AR** ☐ **AV**
Objetivo	**La AC firma los documentos confidenciales (previamente generados) en formato PDF para cada uno de los empleados del sistema. Los documentos tienen un nombre de fichero fijado previamente. Para firmar un documento para un empleado utiliza la clave pública del empleado para cifrar el documento. Y para firmar el documento utiliza la clave privada de la AC.**
Pre-condción	▪ La base de datos está levantada. ▪ El empleado dispone de clave pública para poder cifrar el documento que se le envía. ▪ La AC tiene su clave privada.
Escenario	1. LA AC selecciona la opción "Cifrar documentos". 2. La AC selecciona el documento pdf del empleado que quiere cifrar del formulario cargado. 3. El sistema carga automáticamente los datos relativos al empleado al que va dirigido dicho documento. 4. La AC selecciona el certificado con clave pública del empleado al que va dirigido el documento en el repositorio donde se encuentran todas las claves públicas de los empleados. 5. Se carga el certificado en el formulario. 6. La AC pulsa el botón de "Cifrar Documento" y se producirá un documento cifrado con la extensión de fichero establecida en el fichero .ini 7. La AC pulsa el botón de "Firmar documento" y el sistema selecciona la clave privada de la AC (certificado con extensión .pfx) y realiza la firma de dicho documento.
Escenario Alternativo	**2 a. Si el nombre del documento no cumple el formato establecido no se puede seguir. Volver a 1**
Post-condición	▪ Mensaje que indica como se ha realizado el cifrado. ▪ Mensaje que indica como se ha realizado la firma del documento..

Tabla 3.24: Caso de uso UC-23. Iniciar sesión.

Versión	**1.0**
ID	**UC-23**
Título	**Iniciar sesión.**
Actor	☒ **Empleado** ☒ **AC** ☒ **AR** ☒ **AV**
Objetivo	**Iniciar sesión en el sistema para poder acceder a la funcionalidad de la aplicación según el perfil del usuario.**
Pre-condción	▪ La base de datos está levantada.
Escenario	1. El usuario introduce su nombre y password para validarse en el sistema. 2. Carga el menú principal acorde con sus privilegios.
Escenario Alternativo	▪ Usuario o Contraseña incorrecto. Volver a 1.
Post-condición	**El usuario entra al sistema.**

3.6. Catálogo de Requisitos Software

El objetivo de esta parte de la memoria es la de detallar los requisitos funcionales para poder diseñar nuestra PKI y todos sus componentes. Estos requisitos se dividen en funcionales y no funcionales. Siendo los requisitos funcionales los que indican qué debe ser capaz de realizar el sistema y los segundos especifican cómo se tienen que realizar dichas tareas que fueron especificadas en los primeros. El formato que vamos a utilizar para facilitar la lectura y comprensión de los mismos será el siguiente:

Tabla 3.25: Plantilla de requisitos funcionales.

Identificador	**XX-UR-YY**
Título	
Prioridad	☐ **Alta** ☐ **Media** ☐ **Baja**
Necesidad	
Fuente	
Descripción	

Dónde:

- ***Identificador:*** es el código unívoco que identifica cada requisito
- ***Título:*** es el nombre único del requisito.
- ***Descripción:*** explica la especificación del requisito de manera simple y precisa.
- ***Necesidad:*** establece la importancia del requisito desde el punto de vista del cliente. Los valores pueden ser esencial, conveniente u opcional.
- ***Prioridad:*** establece la importancia del requisito o función del desarrollo del proyecto. Los valores pueden ser alta, media o baja.
- ***Fuente:*** indica la procedencia del requisito.

3.6.1. Requisitos Funcionales del sistema

Estos son los requisitos que tiene que cumplir el sistema que desarrollamos y que indican "qué" tiene que hacer el sistema. Como se ve, todos tienen como fuentes el cliente por lo que su implementación debe ser obligatoria.

Tabla 3.26: RF-01.

Identificador	RF-01
Título	Iniciar Sesión
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El sistema debe permitir iniciar sesión a los usuarios.	

Tabla 3.27: RF-02.

Identificador	RF-02
Título	Cerrar Sesión
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El sistema debe permitir cerrar sesión a los usuarios.	

Tabla 3.28: RF-03.

Identificador	RF-03
Título	Permitir distintos roles
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El sistema tendrá distintos roles o tipos de usarios. Estos serán empleados; AC, AR y AC.	

Tabla 3.29: RF-04.

Identificador	RF-04
Título	Creación de Certificados
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El sistema permitirá la creación de certificados digitales a los empleados de la empresa.	

Tabla 3.30: RF-05.

Identificador	RF-05
Título	Alta de Empleados
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El alta de empleados los realiza la AR .	

Tabla 3.31: RF-06.

Identificador	RF-06
Título	Modificar empleados
Prioridad	☐ Alta ☑ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
La modificación de empleados los realiza la AR .	

Tabla 3.32: RF-07.

Identificador	RF-07
Título	Eliminar empleados
Prioridad	☐ Alta ☑ Media ☐ Baja
Necesidad	Opcional
Fuente	Cliente
Descripción	
La eliminación de un empleado del sistema lo realiza la AR .	

Tabla 3.33: RF-08.

Identificador	RF-08
Título	Solicitud de Certificados
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
Todos los empleados del sistema podrán solicitar la creación de un certificado digital mediante una solicitud a la AR .	

Tabla 3.34: RF-09.

Identificador	RF-09
Título	Verificar Datos
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
La AR verifica que los datos de los empleados son correctos.	

Tabla 3.35: RF-10.

Identificador	RF-10
Título	Generar solicitud de certificado
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
La AR tramitará y gestionará la solicitud de cerfitificado.	

Tabla 3.36: RF-11.

Identificador	RF-11
Título	Respuesta de solicitud
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
La aprobación o rechazo de solicitudes de certificados es realizada por la AR .	

Tabla 3.37: RF-12.

Identificador	RF-12
Título	Notificar a la AC
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
La AR es la encargada de notificar a la AC la aceptación o denegación de las solicitudes de los empleados.	

Tabla 3.38: RF-13.

Identificador	RF-13
Título	Revocar los certificados
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
La AC es la encargada de revocar un certificado de la PKI .	

Tabla 3.39: RF-14.

Identificador	RF-14
Título	Ciclo de vida del certificado
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El sistema debe ser capaz de mostrar el ciclo de vida de un certificado. (AV)	

Tabla 3.40: RF-15.

Identificador	RF-15
Título	Verificar certificado
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El sistema debe ser capaz de verificar el estado y la validez de un certificado. (AV)	

Tabla 3.41: RF-16.

Identificador	RF-16
Título	Mostrar la lista CRL
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El sistema debe ser capaz de mostrar la lista CRL en vigor. (AC)	

Tabla 3.42: RF-17.

Identificador	RF-17
Título	Búsqueda de Certificados Revocados
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El sistema debe ser capaz de realizar la búsqueda de certificados revocados. (AC)	

Tabla 3.43: RF-18.

Identificador	RF-18
Título	Identificación de Certificados
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
Cada certificado emitido por la PKI debe tener un número de serie único.	

Tabla 3.44: RF-19.

Identificador	RF-19
Título	Firmar documentos
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El sistema debe ser capaz de firmar documentos para garantizar la integridad y no repudio en origen.	

Tabla 3.45: RF-20.

Identificador	RF-20
Título	Solicitar Revocación de Certificado
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El sistema debe permitir que un empleado pueda solicitar la revocación de su certificado.	

Tabla 3.46: RF-21.

Identificador	RF-21
Título	Cifrar documentos
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
Los empleados del sistema podrán cifrar documentos entre ellos.	

Tabla 3.47: RF-22.

Identificador	RF-22
Título	Descifrar documentos
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El sistema de debe ser capaz de descifrar documentos previamente cifrados.	

Tabla 3.48: RF-23.

Identificador	RF-23
Título	Certificados Digitales
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
El sistema utilizará los certificados generados por la PKI para firmar, descifrar, firmar y verificar firmas.	

3.6.2. Requisitos No Funcionales del sistema

En este apartado se especifican los requisitos no funcionales del sistema que sirven para complementar a los requisitos funcionales del apartado anterior y hacen referencia al "cómo" se tienen que implementar en el sistema.

Tabla 3.49: RNF-01.

Identificador	RNF-01
Título	Clave Pública y privada
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
Cada empleado del sistema que disponga de un certificado de la PKI dispondrá de dos ficheros uno con extensión ".cer"que contendrá su clave pública y otro con la extensión “.pfx” que contendrá su clave privada.	

Tabla 3.50: RNF-02.

Identificador	RNF-02
Título	Formato Certificado Digital
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
Los certificados generados por la PKI del sistema cumplen con el estándar internacional ITU-T X.509.	

Tabla 3.51: RNF-03.

Identificador	RNF-03
Título	Versión de los certificados
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
La versión de los certificados generados en el sistema es 3.	

Tabla 3.52: RNF-04.

Identificador	RNF-04
Título	Certificado AC
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
La creación del certificado de la AC tanto el que contiene la clave pública como el que contiene la clave privada es previo a la generación de cualquier certificado de un empleado.	

Tabla 3.53: RNF-05.

Identificador	RNF-05
Título	Formato de los documentos del sistema
Prioridad	☑ Alta ☐ Media ☐ Baja
Necesidad	Esencial
Fuente	Cliente
Descripción	
Todos los documentos que cifra y firma la Ac deben estar previamente generados y tienen que tener el siguiente formato en su nombre de fichero: YY-MM-XX-ZZZZZZ.pf. Donde YY es el año de creación del documento, MM es el mes de creación del documento, XX es el tipo de documento al que pertenece y ZZZZZZ es id de empleado al que va dirigido.	

Capítulo 4

Diseño del Gestor de Certificados

Una vez realizado el análisis del proyecto a realizar procedemos a realizar el diseño de la solución a implementar. En el apartado 4.1 mostraremos el modelo de datos que utilizaremos, junto con la definición de las tablas que lo forman. También mostraremos las interfaces de usuario. En el apartado 4.4 se expondrá el diseño de interfaces de usuario que sirve para explicar de qué forma se ha llevado a cabo el diseño de las interfaces de usuario.

4.1. Elaboración del modelo de datos

En este apartado queremos mostrar el modelo de datos utilizado para la implementación del sistema creado y la importancia de dicho modelo para el correcto funcionamiento de la PKI, así como la parte de la aplicación que se ejecuta en los equipos de cada empleado.

Este modelo se basa en unas entidades fundamentales como son los certificados, empleados y CRL. En torno a estas tres, se rige todo el modelo. Con empleados queremos tener la información de todos los usuarios del sistema y su relación con los certificados que poseen. También esta entidad está relacionada con las solicitudes de certificados que haga un empleado, los documentos asociados que tiene dicho empleado y su relación con la identificación que tiene que hacer un empleado para acceder al sistema.

Otra entidad fundamental es la de certificados, que es el motor de la PKI y donde se registran todos los certificados del sistema, los estados por los que va pasando en función de la operación que se haga con ellos y que permite realizar un ciclo de vida completo del mismo.

La otra gran entidad del sistema es la CRL que es la que se encarga de gestionar los certificados revocados que se produzcan. Ésta está en relación con los empleados a los que pertenece el certificado y el certificado en sí que se va a revocar.

Es importante señalar que la entidad CRL es la que utiliza la AV para mostrar en el sistema la CRL de la PKI. En teoría la CRL debería estar publicada en una web donde los usuarios se la pueden descargar y consultar en esa lista si el certificado esta revocado o no. Nosotros no lo hemos implementado así y lo hacemos a través de un formulario Windows que se conecta a la base de datos para obtener dicha información. Permite eso sí, la consulta de cualquier certificado para saber si esta revocado y lo mismo para cualquier CRL.

También hay que mencionar que es diseño está hecho para nuestro caso concreto que

queremos garantizar la confidencialidad de documentos de una empresa, en este caso hemos optado por implementar un tipo de esos documentos posibles como puede ser la nómina, si bien a la hora de adaptarlo a otros escenarios habría que crear las tablas correspondientes a dichos documentos que queremos guardar.

Además tenemos una serie de tablas que nos sirven para garantizar las gestiones de solicitudes de certificados y revocación de las mismas y los estados por los que van pasando tanto las solicitudes como los propios certificados.

Todo esto es posible realizarlo gracias a la BD y el acceso de la aplicación a dicha información. La imagen del modelo de la base de datos en un formato más visible ha sido agregada como Anexo A (A).

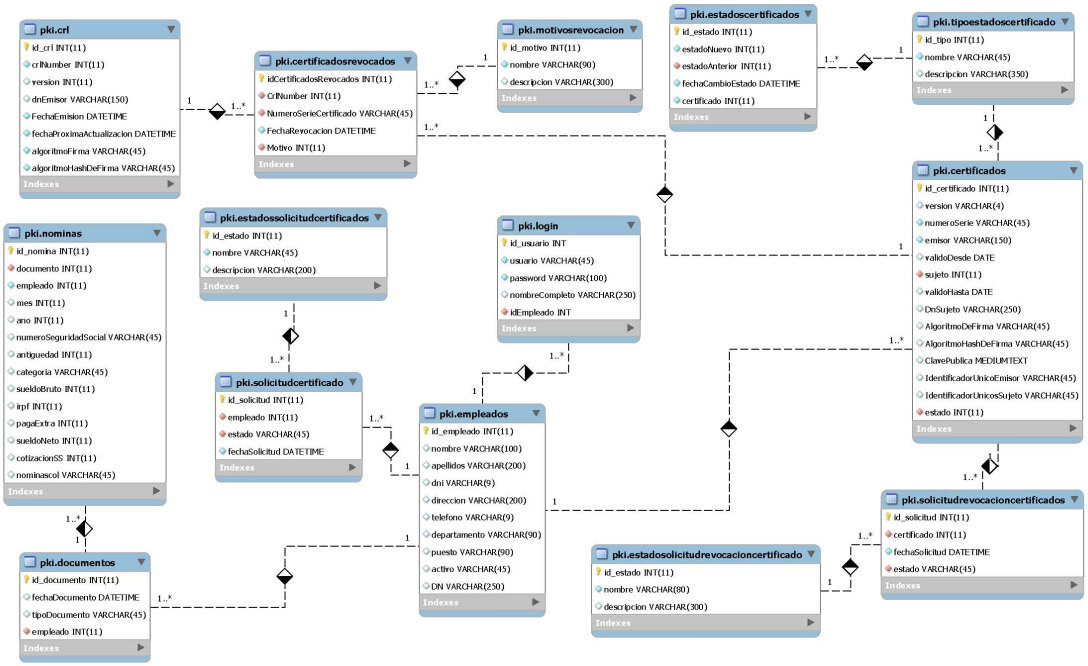


Figura 4.1: Modelo de datos del Sistema.

4.1.1. Diccionario de datos

Supuestos semánticos:

- Cada empleado de nuestro sistema sólo puede tener un certificado.
- Un documento del sistema (nómina...) solo puede pertenecer a un empleado.
- Cada documento del sistema solo puede pertenecer a un tipo de documento.
- Un certificado revocado solo puede pertenecer a una única CRL .

Las tablas que forman parte de nuestro modelo datos son las siguientes:

- **Certificados** ⇒ tabla que contiene toda la información relativa de un certificado del empleado.
- **tipoEstadosCertificados** ⇒ tabla que recoge los diferentes estados por los que puede pasar un certificado.
- **estadosCertificados** ⇒ tabla que sirve para almacenar los diferentes estados por los que ha pasado un certificado.
- **motivosRevocacion** ⇒ tabla que recoge los motivos por los que se puede revocar un certificado.
- **certificadosRevocados** ⇒ tabla que sirve para almacenar los certificados que han sido revocados y que se encuentran en una CRL .
- **CRL** ⇒ tabla que almacena la información de una CRL del sistema.
- **Empleados** ⇒ tabla que almacena la información de los empleados del sistema.
- **Login** ⇒ tabla que almacena que sirve para validar un usuario en el sistema.
- **solicitudCertificado** ⇒ tabla que recoge la información de las solicitudes de certificados de los empleados.
- **estadosSolicitudCertificados** ⇒ tabla que recoge los distintos estados por los que pasa una solicitud de certificado.
- **Documentos** ⇒ tabla que indica el tipo de documento que esta en el sistema.
- **Nominas** ⇒ tabla que almacena la información de las nóminas de los empleados del sistema.
- **solicitudRevocaciónCertificados** ⇒ tabla que almacena las diferentes solicitudes de revocación de certificados.
- **estadosSolicitudRevocacionCertificado** ⇒ tabla que guarda los diferentes estados por los que puede pasar una solicitud de revocación de certificado.

A continuación pasaremos a definir los campos de cada una de ellas.

Tabla: certificados

Es junto con empleados las tablas más importantes de la base de datos. En ella guardamos la información de cuando se crea físicamente el certificado en la base de datos y el empleado al que pertenece. Si bien antes de que se cree físicamente, la AR acepta la solicitud de certificado del empleado y se crea un registro nuevo aunque sin los datos definitivos de dicho certificado. Se cargan solo los datos del número de serie, emisor, sujeto y estado "Pre-activado". Después, cuando la AC autorice dicha creación de certificado se cargaran todos los datos de la tabla y se pasará a estado "Activado". Los campos de la tabla son:

- **id_certificado** ⇒ clave primaria de la tabla y que identifica unívocamente a un certificado, al igual que el número de serie.
- **Version** ⇒ versión de certificado creado. Todos serán de tipo 3.
- **numeroSerie** ⇒ numero de serie del certificado, cuyo valor debe ser único para cada uno de los certificados generados.

- **Emisor** ⇒ identifica al nombre de la AC que lo ha generado, que es la emisora de los certificados.
- **Sujeto** ⇒ empleado al que pertenece el certificado digital.
- **validoDesde** ⇒ fecha a partir de la cual el certificado esta en vigor.
- **validoHasta** ⇒ fecha a partir de la cual el certificado deja de estar en vigor y pasa a estar expirado.
- **dnSujeto** ⇒ "distinct name"del sujeto. Esta formado por el nombre+apellidos+dni
- **AlgoritmoteDeFirma** ⇒ algoritmo utilizado para firmar el certificado.
- **AlgoritmoHashDeFirma** ⇒ algoritmo de firma que ha utilizado la AC para firmar el certificado.
- **ClavePublica** ⇒ clave publica del certificado.
- **IdentificadorUnicoEmisor** ⇒ identificador que identifica unívocamente al emisor del certificado.
- **dentificadorUnicoSujeto** ⇒ identificador que identifica unívocamente al titular del certificado.
- **Estado** ⇒ estado del certificado en el sistema.

Sus relaciones con el resto de tablas se pueden ver en el diseño del modelo de la base de datos mostrado anteriormente.

Tabla: tipoEstadosCertificados

Tabla que utilizamos para reflejar en el sistema los diferentes estados por los que puede ir pasando un certificado desde que se crea hasta que expira o se revoca. Los campos de dicha tabla son:

- **id_certificado** ⇒ identificador único de cada tipo de estado de certificado.
- **Nombre** ⇒ nombre del estado del certificado.
- **Descripción** ⇒ descripción ampliada del nombre del estado del certificado.

Tabla: estadosCertificados

Tabla que sirve para guardar los diferentes estados por los que va pasando un certificado a lo largo del tiempo y poder realizar por tanto un ciclo de un certificado concreto. Los campos de la tabla son:

- **id_estado** ⇒ identifica unívocamente un estado.
- **estadoNuevo** ⇒ estado al que cambia un certificado.
- **estadoAnterior** ⇒ estado que tenía el certificado antes del cambio.

- **fechaCambioEstado** ⇒ fecha en la que se produce el cambio de estado del certificado.
- **Certificado** ⇒ certificado que cambia de estado.

Tabla: motivosRevocacion

Tabla que contiene los diferentes motivos por los que se puede revocar un certificado. La tabla tiene los siguientes campos:

- **id_motivo** ⇒ identificador único del motivo de revocación.
- **Nombre** ⇒ motivo de revocación de un certificado.
- **Descripción** ⇒ descripción del motivo de revocación.

Tabla: certifcadosRevocados

Tabla que contiene todos los certificados revocados que se han producido en nuestro sistema. El revocar un certificado es un hecho irreversible, por lo que el ciclo de vida del certificado termina ahí. La tabla tiene los siguientes campos;

- **idCertificadosRevocados** ⇒ identificador único del certificado revocado
- **CrlNumber** ⇒ número de la CRL en la que el certificado revocado se encuentra incluido.
- **NumeroSerieCertificado** ⇒ número de serie del certificado revocado
- **fechaRevocacion** ⇒ fecha en a que se ha producido la revocación del certificado.
- **Motivo** ⇒ motivo de la revocación del certificado.

Tabla: CRL

Tabla que representa la lista de revocación de certificados del sistema. Solo puede haber una lista activa en una PKI . Esta lista esta formada por todos los certificados que se han revocado mientras esta vigente. La tabla contiene los siguientes campos:

- **id_crl** ⇒ identificador único de la CRL.
- **crlNumber** ⇒ Número de la CRL .
- **version** ⇒ versión de la CRL .
- **dnEmisor** ⇒ el nombre de la entidad emisora. La AC (será "$CA\_GesCert$").
- **FechaEmision** ⇒ fecha en la que se ha creado la CRL y empieza a estar activa.
- **fechaProximaActualización** ⇒ fecha hasta cuando esta en vigor la CRL

- **algoritmoFirma** ⇒ algoritmo de firma de la CRL.
- **algoritmoHashDeFirma** ⇒ algoritmo hash con el que se ha firmado la CRL

Tabla: Empleados

Tabla que contiene la información de los empleados del sistema. Esta tabla la creará y la gestionará la AR. La tabla contiene los siguientes campos:

- **id_empleado** ⇒ Identificador único del empedado.
- **Nombre** ⇒ Nombre del empleado.
- **Apellidos** ⇒ Apellidos del empleado.
- **Dni** ⇒ DNI del empleado.
- **Teléfono** ⇒ Teléfono del empleado.
- **Departamento** ⇒ Departamento al que pertenece el empleado.
- **Puesto** ⇒ Puesto dentro del departamento que ocupa el empleado.
- **Activo** ⇒ Indica si el empleado se encuentra en activo en la empresa o ha sido dado de baja.
- **Dn** ⇒ Distinct Name del empleado. Esta formado por el nombre+apellidos+dni.

Tabla: Login

Tabla que sirve para validar a los usuarios del sistema. En el campo password se almacena el valor hash del password. La tabla contiene los siguientes campos:

- **id_usuario** ⇒ identificador único del usuario.
- **Usuario** ⇒ nombre de usuario en el sistema. Son las iniciales del nombre y apellidos.
- **Password** ⇒ valor hash del password que introduce el usuario.
- **nombreCompleto** ⇒ Nombre completo del usuario.
- **idEmpleado** ⇒ tabla de empleado al que pertenece el usuario.

Tabla: solicitudCertificado

Tabla que contiene la información de las solicitudes de certificados de los empleados. Esta solicitud se envía a la AR. La tabla contiene los siguientes campos:

- **id_solicitud** ⇒ identificador único de la solicitud.
- **empleado** ⇒ empleado que solicita el certificado.
- **estado** ⇒ estado en el que se encuentra la solicitud.
- **fechaSolicitud** ⇒ fecha en la que se realiza la solicitud.

Tabla: estadosSolicitudCertificados

Tabla donde guardan los diferentes estados por los que pueden pasar las solicitudes de certificados. La tabla contiene los siguientes campos:

- **id_estado** ⇒ identificador único del estado de solicitud de certificado.
- **nombre** ⇒ nombre de la solicitud de certificado.
- **descripción** ⇒ descripción de la solicitud de certificado.

Tabla: Documentos

Tabla que recoge los diferentes tipos de documentos del sistema. La tabla contiene los siguientes campos:

- **id_documento** ⇒ identificador único del tipo de documento.
- **fechaDocumento** ⇒ fecha de creación del documento.
- **tipoDocumento** ⇒ tipo de documento del sistema.
- **empleado** ⇒ empleado al que pertenece el documento.

Tabla: Nominas

Tabla que utilizamos para almacenar las nóminas de los empleados del sistema. Es uno de los diferentes tipos de documentos, pero que utilizares como ejemplo para el análisis y diseño del sistema. La tabla contiene los siguientes campos:

- **id_nomina** ⇒ identificador único de la nomina de un empleado.
- **documento** ⇒ tipo de documento al que pertenece.
- **empleado** ⇒ empleado al que pertenece la nómina.
- **mes** ⇒ mes en que se produce la nómina
- **año** ⇒ año en que se ha producido la nómina.

- **numeroSeguridadSocial** ⇒ número de la seguridad social del empleado.
- **antigüedad** ⇒ antigüedad del empleado en la empresa.
- **categoria** ⇒ categoría profesional del empleado.
- **sueldoBruto** ⇒ sueldo bruto del empleado.
- **irpf** ⇒ irpf que se le aplica al empleado en la nómina.
- **pagaExtra** ⇒ paga extra el empleado en la nómina.
- **sueldoNeto** ⇒ sueldo neto del empleado.
- **cotizacionSSs** ⇒ cotización del empleado a la Seguridad social

Tabla: solicitudRevocaciónCertificados

Tabla que almacena las distintas solicitudes de revocación de certificados de los empleados. La tabla contiene los siguientes campos:

- **id_solicitud** ⇒ identificador único de la solicitud de revocación del empleado.
- **certificado** ⇒ certificado que se va a revocar.
- **fechaSolicitud** ⇒ fecha de la solicitud de revocación.
- **estado** ⇒ estado de la solicitud de la revocación.

Tabla:estadosSolicitudRevocacionCertificado

Tabla donde recogemos el estado de las solicitudes de certificados. La tabla contiene los siguientes campos:

- **id_estado** ⇒ identificador único del estado de una solicitud de revocación de certificado.
- **nombre** ⇒ nombre del estado de la solicitud de la revocación del certificado.
- **descripción** ⇒ descripción detallada del estado de revocación del certificado.

4.2. Definición de interfaces de usuario

- ***Diagrama de navegación – Aplicación PKI***
  En este apartado se va a mostrar un diagrama de navegación de la aplicación PKI con el objeto de mostrar la navegabilidad entre las distintas pantallas que contiene la aplicación.

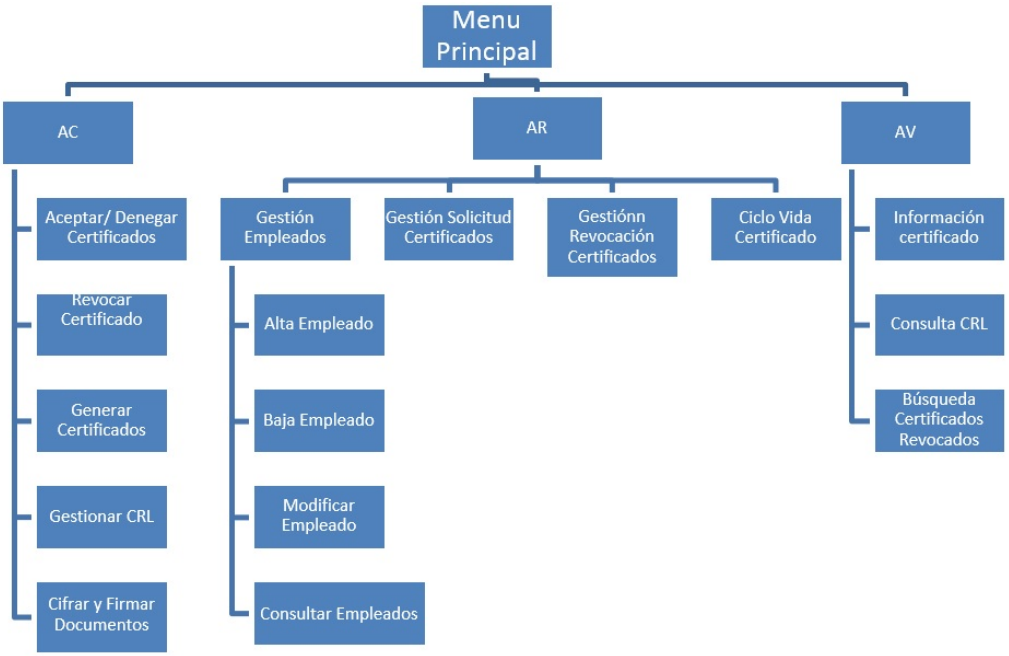


Figura 4.2: Diagrama de navegación – aplicación PKI.

- ***Diagrama de navegación – Aplicación empleado.***
  A continuación mostramos el diagrama de navegación de la aplicación de los empleados, con el objeto de mostrar la navegabilidad entre las distintas pantallas que contiene la aplicación.

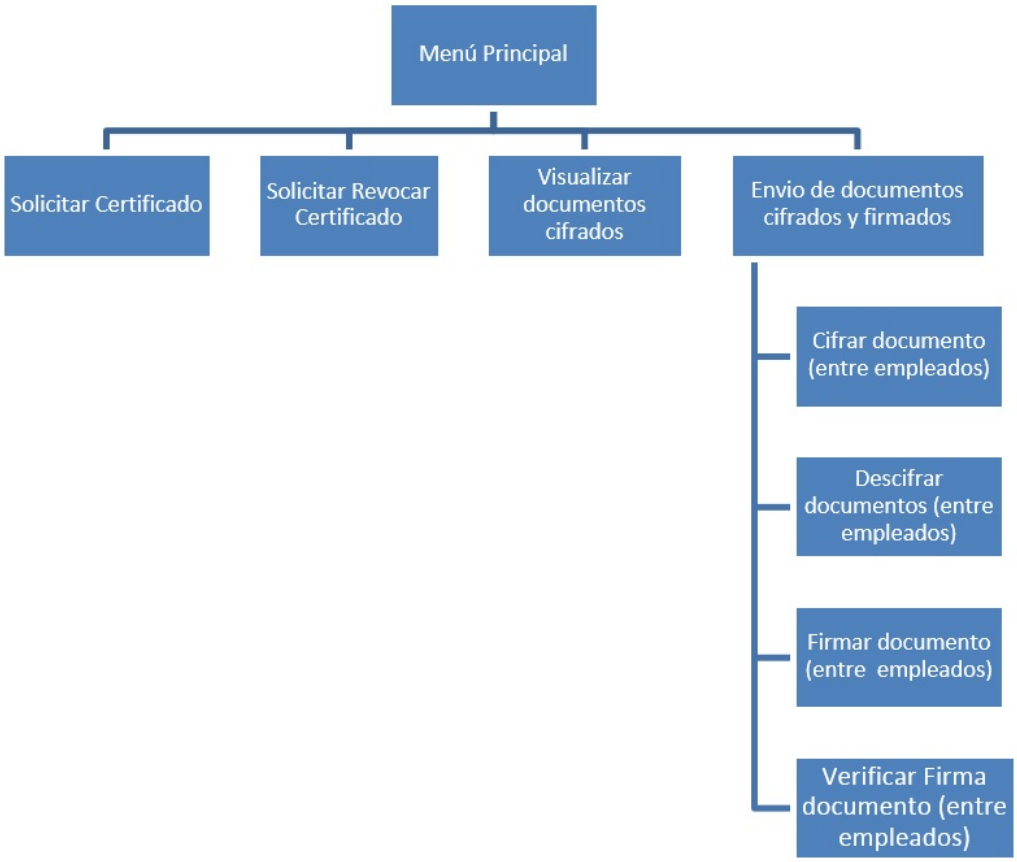


Figura 4.3: Diagrama de navegación – aplicación empleado.

4.3. Arquitectura definitiva

En la arquitectura definitiva hemos optado por dividir en dos aplicaciones en función si es la aplicación que van a utilizar los empleados o es la aplicación que simula la PKI. Ambas aplicaciones compartirán la misma base de datos. Siendo la aplicación de los empleados ejecutada desde cada equipo del usuario y la que simula la PKI alojarla en un servidor. Cada empleado tendrá en su equipo la aplicación de empleados, así como su certificado instalado en su equipo para poder trabajar correctamente con dicha aplicación. Esto lo hemos decidido al realizar el análisis y diseño del proyecto y vimos que en realidad eran independientes y se podían separar.

4.4. Descripción de la Interfases Gráficas de la Aplicación

Una vez descrito de forma general el diseño metodologico de la aplicación, en este apartado pasamos a explicar ciertos aspectos correspondientes a las interfases de los diferentes usuarios que interactúan con la aplicación. Como en los capítulos anteriores se ha descrito, la aplicación consta de dos perspectivas funcionales; la primera es la perspectiva de un PKI y una segunda que es la perspectiva de un Empleado. Inicialmente empezaremos con describir de manera general algunas de las principales interfases gráficas en la que la aplicación permitira la interacción de los diferentes usuarios descritos previamente desde la perspectiva de una PKI, para posteriormente describir de manera general las interfases

gráficas desde la perspectiva funcional del Empleado.

4.4.1. Interfase de la Aplicación desde la perspectiva PKI

Como hemos indicado a lo largo de la memoria, queremos implementar la simulación de una pequeña PKI con sus componentes fundamentales. Pues bien, para ellos en el diseño de la aplicación hemos supuesto que la aplicación va a ser utilizada por 3 tipos de usuario diferentes que harán las funciones de AC, AR y AV.

Entonces tendríamos la aplicación PKI con el siguiente menú principal para AR.

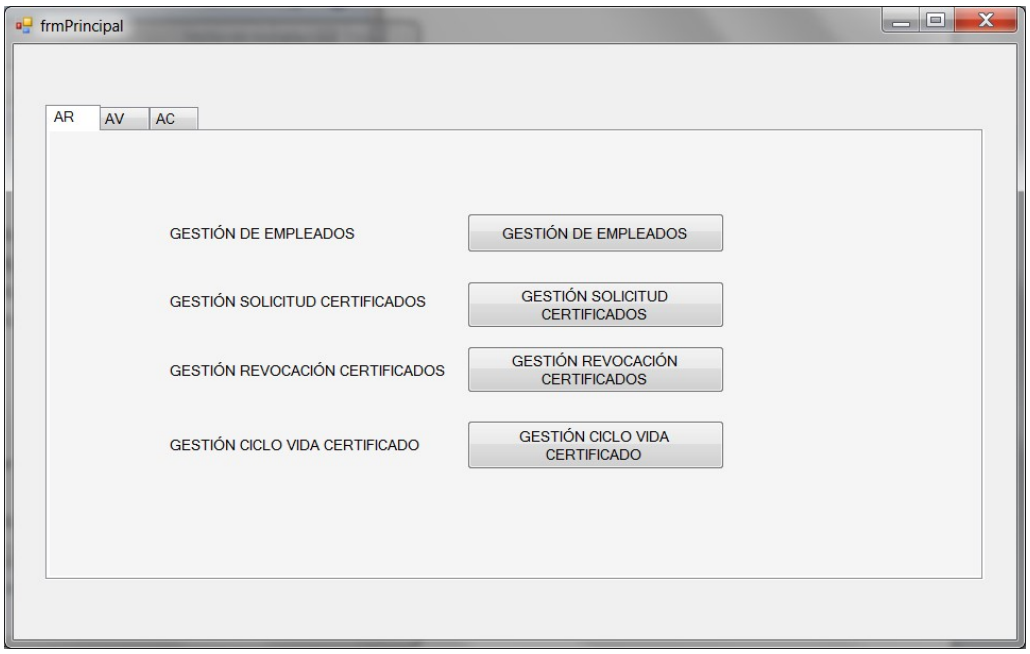


Figura 4.4: Menu principal de la Interfase de la aplicación para el usuario AR.

Al pinchar sobre la pestaña "AV", nos posicionaríamos en la opción que simula al usuario de una Autoridad de Verificación como se muestra en la Figura 4.5.

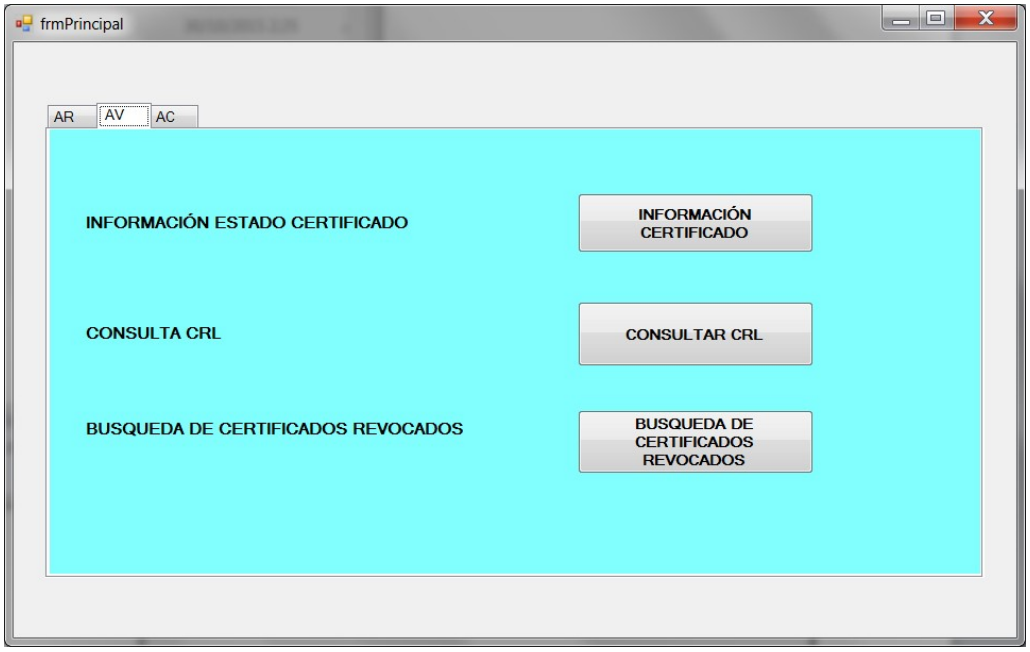


Figura 4.5: Menu principal de la Interfase de la aplicación para el usuario AV.

Como se muestra en la Figura 4.5, hemos querido llamar la atención del usuario al implementar diferentes colores de fondo de pantalla con relación a cada usuario del sistema. Por eso en la Figura 4.5 el fondo de pantalla del usuario AV es magenta en comparación con el usuario AR en la Figura 4.4.

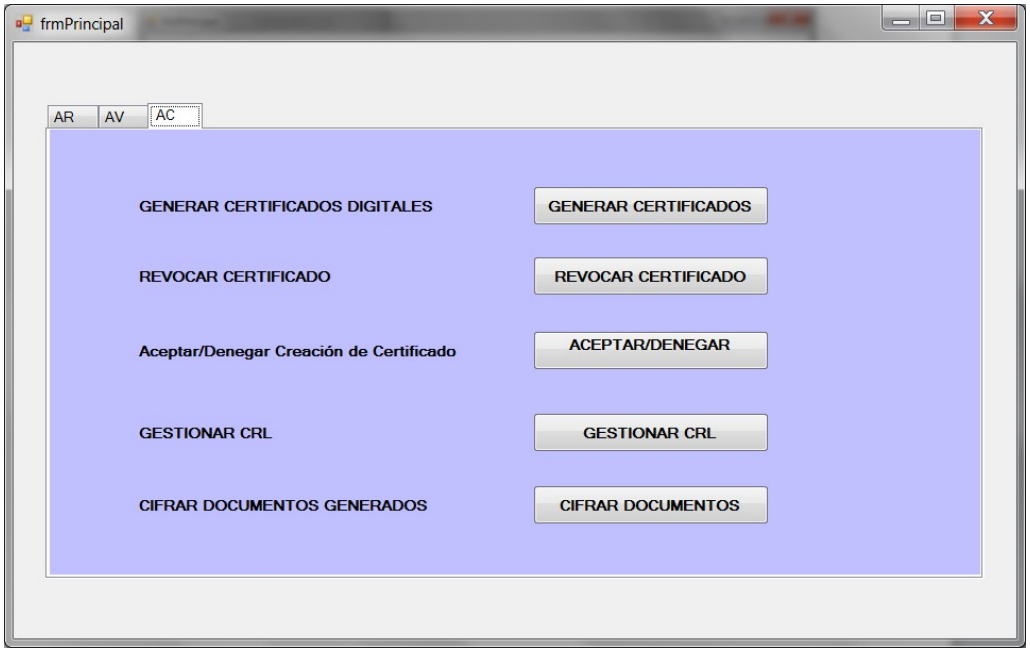


Figura 4.6: Menu principal de la Interfase de la aplicación para el usuario AC.

Siguiendo la misma lógica de colores para cada usuario, en la Figura 4.6 para el usuario "AC" se muestra la interfase de la aplicación en un color diferente a los usuarios anteriores.

Además en esta misma Figura 4.6, se puede observar las diferentes opciones de interacción con el sistema para el usuario mencionado.

4.4.1.1. Autoridad de Certificación (AC)

Esta parte de la interfase de la aplicación que es manipulada por el usuario correspondiente para simular el comportamiento de la Autoridad de Certificación (AC) de la PKI.

Como puede verse cada usuario tiene definidas claramente las funciones que realiza.

Para explicarlo más claro lo vamos a numerar de la siguiente manera:

1. **AC ⇒ Generar Certificados.**
2. **AC ⇒ Revocar Certificado.**
3. **AC ⇒ Aceptar / Denegar.**
4. **AC ⇒ Gestionar CRL.**
5. **AC ⇒ Cifrar Documentos.**

Pasamos a analizar en profundidad cada una de ellas. Comenzamos por la AC que es la principal y la que tiene más complejidad.

1. El primer elemento es **"Generar Certificados"**, si pulsamos sobre el botón nos mostrará el formulario que se encarga de crear un certificado de un empleado.
   Nota: Hay que comentar, que previamente a poder generar los certificados la AC ha emitido su propio certificado firmado en este caso por ella misma, es lo que se denomina **self signed**. Este certificado es lo que se denomina **certificado raíz**. La clave pública del certificado raíz al igual que la clave pública de los certificados de los empleados debe ser pública y accesible para todos los elementos del sistema. Este certificado de la AC se llamará **CACertGes**.

   El formulario por tanto es el siguiente:

Figura 4.7: Formulario para la creación de certificados.

Donde en primer lugar la AC debe introducir en el campo "DNI del Empleado a Generar Certificado" su DNI, que debe estar registrado en la base de datos de empleados y que debe haber solicitado previamente una solicitud de creación de certificado.

Una vez introducido el DNI pulsará el botón de "Buscar" y se mostraran en la parte central del formulario los datos del empleado que solicito el certificado y cuyo estado es "Pre-activado".

Figura 4.8: Resultado de la interacción al crear un certificado.

A continuación tendrá que rellenar el resto de campo del grupo "Datos del certificado" como son la fecha comienzo y fin de periodo de validez del certificado, donde se va a ubicar el certificado, en que almacén de certificados, la longitud de la clave del certificado, el algoritmo de firma utilizado para firmar el certificado por la AC.

Como resultado obtenemos dos ficheros uno con extensión .cer que contiene la clave pública del empleado y otro con extensión .pfx que contiene la clave privada del empleado. (Esta clave se puede proteger con una contraseña que pide al crearse, también se puede dejar en blanco, esta es la opción que hemos elegido para simplificar el proceso).

Este certificado creado está firmado por la Ac que hemos creado inicialmente (recordar que la función de un certificado es garantizar la vinculación entre la identidad del sujeto y su clave pública. Por tanto CACertGes firma el contenido del certificado generado.

Además se encarga de actualizar la tabla de certificados de la base de datos dejándolo en estado "Emitido" e insertando también en la tabla que guarda los estados por los que va pasando un certificado, que es "estadoscertificados".

Por tanto al terminar de ejecutar el empleado tendrá su clave pública y privada, y entonces tendrá que guardar en un lugar seguro el fichero con extensión .pfx y el que tiene extensión .cer colocarlo donde están el resto de claves públicas de los empleados del sistema.

2. Pasamos ahora a la opción del menu del usuario AC de **"Revocar Certificado"**, mediante la cual la AC puede revocar un certificado que el empleado ha solicitado previamente a través de la AR y que nos muestra el estado en que se encuentran dichas solicitudes. Nos permite filtrar por solicitudes aceptadas, en trámite o simplemente mostrar todos los certificados del sistema. El formulario seria como el siguiente:

Figura 4.9: Resultado de la acción **"Revocar Certificado"**

.

Para revocarlo por tanto la AC seleccionará de la lista de certificados el o los certificados que quiera y seleccionará el motivo de revocación de la lista que se encuentra en la parte inferior izquierda y a continuación pulsar el botón de "Revoc
ar Certificado".

El sistema se encarga de cambiar el estado del certificado a "Revocado", insertarlo en la lista activa de revocación de certificados (CRL), insertar en las tablas que guardan los estados de los certificados y en la lista que guardan la solicitudes de revocación de certificados.

3. La siguiente opción del menú principal para el usuario AC es **"Aceptar/Denegar"** que encarga de aprobar o denegar las solicitudes que la AR le transmite sobre la creación de certificados, tanto las aceptadas como las denegadas. Para ello tenemos que marcar en la lista de "solicitudes aceptadas" los certificados que queremos aceptar y pulsar el botón de "Aceptar solicitudes" o en la otra lista que está debajo "solicitudes denegadas" y pulsar el botón "Denegar solicitudes".

   Si es una solicitud aceptada se creará un certificado con estado "Pre-activado" y asignándole un número de serie pero sin indicar la fecha desde la cual está vigente, esto se hace en la opción anterior "generar certificado". Si lo que queremos es denegar una solicitud de certificado lo que se hace es borrar de la base de datos la solicitud de creación de certificado del empleado.

   El formulario que muestra esta opción es el siguiente:

Figura 4.10: Gestion de **"Aceptar/Denegar"** en la creación de certificados.

4. Otra opción más de la Ac es **"Gestionar CRL"** que se encarga de crear una nueva lista de revocación de certificados o bien de añadir un certificado como revocado y asociarlo a la lista de revocación activa en ese momento. Solo puede haber una lista

de revocación activa en un momento dado.

Para crear una nueva CRL tenemos que introducir la fecha de emisión de la lista y la fecha hasta la cual estará vigente, en el campo de fecha de próxima actualización y el algoritmo con el que se va a firmar dicha lista, a continuación pulsar el botón "Crear CRL" y ya tenemos una nueva lista CRL, en este caso sin ningún certificado revocado, hasta que se vayan añadiendo nuevos elementos a dicha lista.

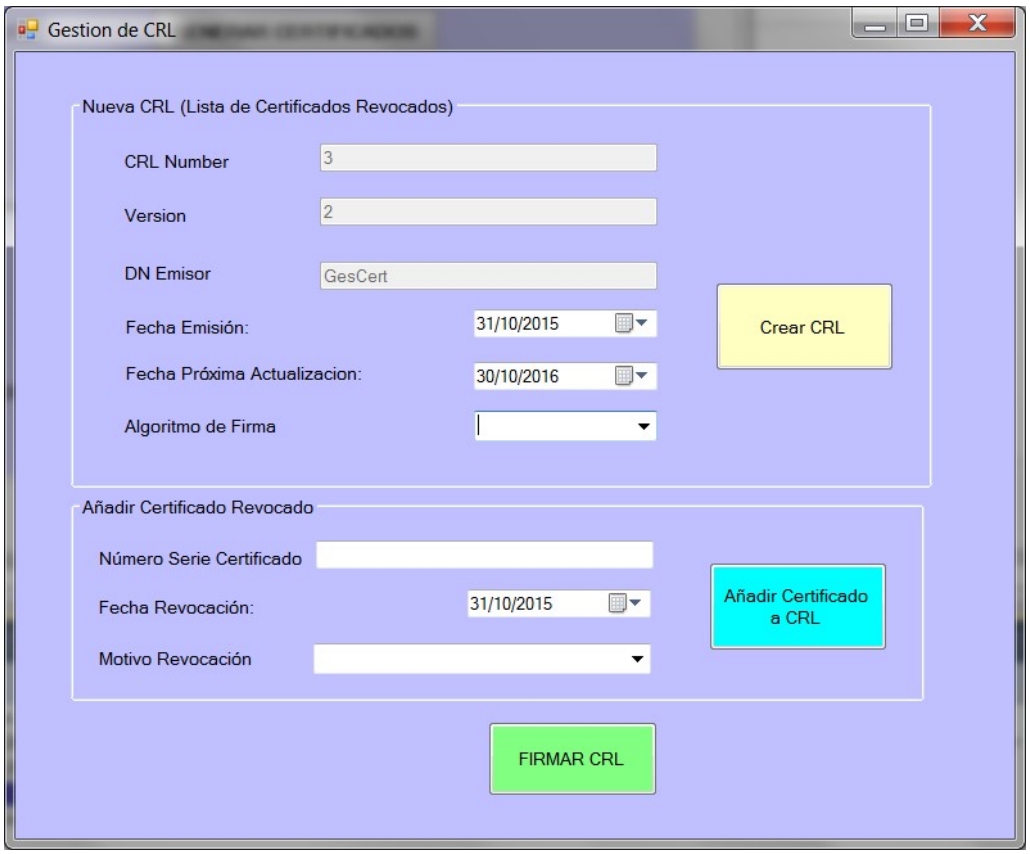


Figura 4.11: Interfase para la Gestión del Control de la lista de Revocación.

Si en cambio, queremos añadir un nuevo certificado revocado a la CRL que está activa tenemos que situarnos en la parte inferior del formulario e introducir el número de serie del certificado, la fecha en la que se va a revocar y por último el motivo de revocación. Pulsamos el botón "Añadir Certificado a CRL" y ese certificado estará en estado revocado y añadido a la CRL.

El botón que aparece en la parte inferior del formulario "FIRMAR CRL" sirve para crear una firma con el contenido de la CRL junto con sus certificados revocados con la clave privada de la AC, y que cualquier empleado se lo pueda descargar (situarlo en una carpeta donde tengan acceso común todos los empleados similar a donde están las claves públicas de éstos) y que después ellos puedan verificar que la firma es correcta, descifrándolo con la clave pública de la AC. Es decir, crearíamos una estructura de datos que represente a la CRL con sus certificados revocados, esta estructura la instanciaremos en un objeto CRL y a continuación firmamos ese objeto

con la clave privada de la AC, (CACertGes).

Un empleado para verificar el contenido de la firma, tendría que descifrar dicho contenido con la clave pública de la AC, obteniendo el valor hash que firmo la AC y comparar por otro lado el que obtendría él aplicando el mismo algoritmo hash o resumen al objeto CRL, si ambos valores coinciden puede estar seguro de la autenticidad de la lista CRL, en caso contrario la lista ha sido modificada.

5. La última opción de la parte de la aplicación referente a la AC es la de **"Cifrar Documentos"** que una de las partes fundamentales de la aplicación ya que se encarga de cifrar el contenido de los documentos que la empresa quiere aumentar el nivel de seguridad.

   El formulario que realiza dicha función es el siguiente:

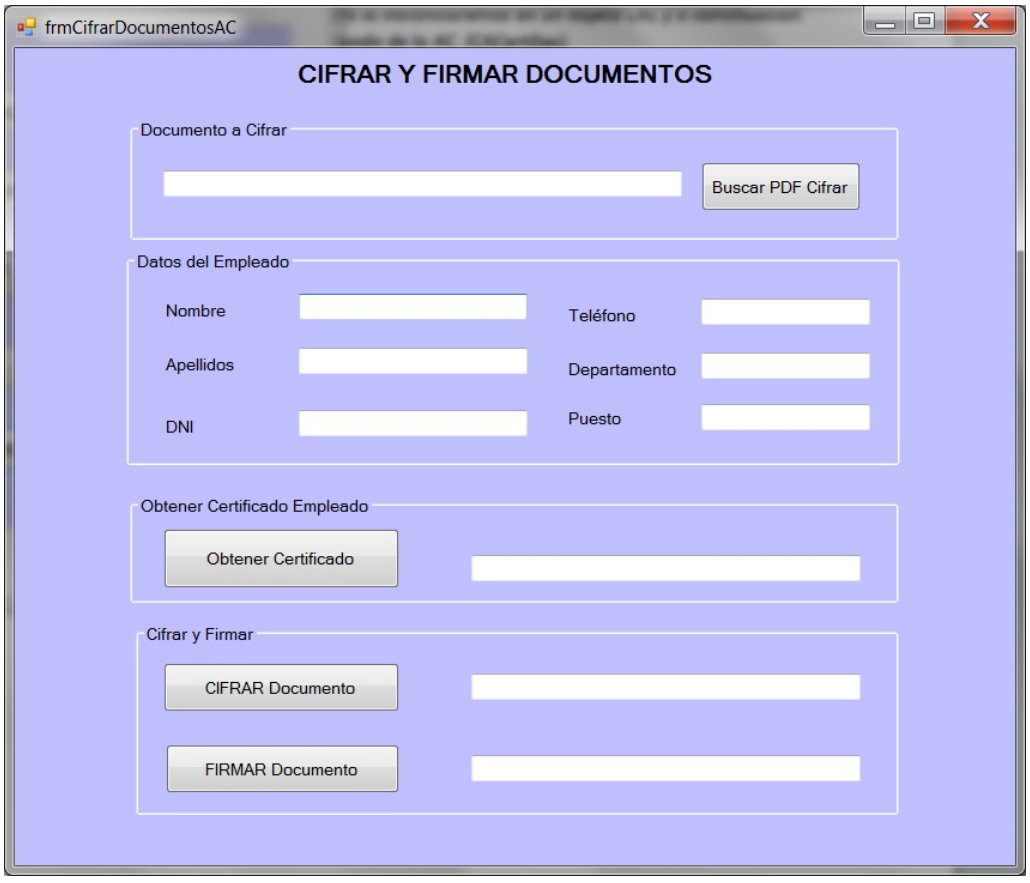


Figura 4.12: Interfase de la aplicación sobre el Cifrado y Firmado de Documentos.

En este formulario lo primero que tenemos que hacer es pulsar el botón "Buscar PDF Cifrar" para buscar el pdf o documento que queremos cifrar. Hay que mencionar que la estructura de los documentos del sistema para poder cifrarse es XX-YY-ZZ-TTTTTT.pdf donde XX e YY es el año y mes respectivamente de la creación del documento, ZZ es el tipo de documento del que forma parte el pdf y TTTTTT es el número de empleado al que pertenece el documento.

Al seleccionar por tanto el documento el sistema carga automáticamente los datos del empleado al que pertenecen en la región del formulario justo debajo de donde selecciona el documento a cifrar, tal como muestra la figura:

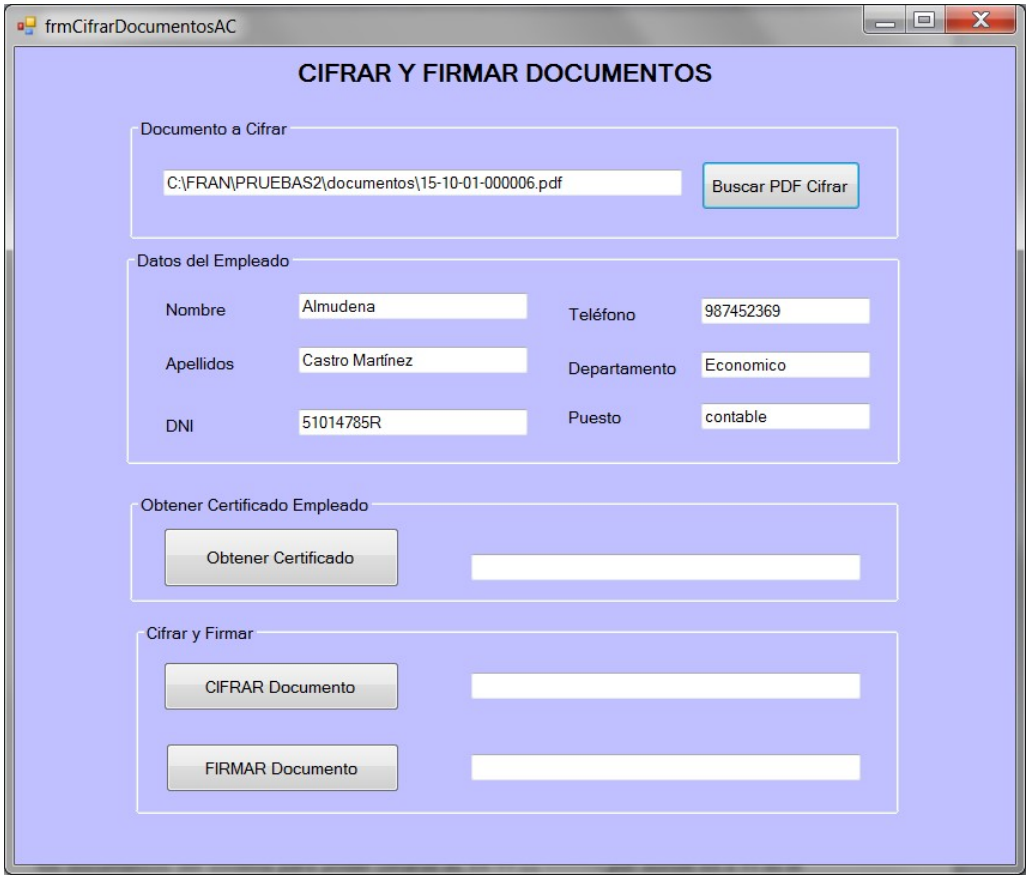


Figura 4.13: Resultados simulados sobre el Cifrado y Firmado de Documentos.

A continuación tenemos que seleccionar la clave pública del empleado con la que la AC va a cifrar el documento. Para ellos pulsamos el botón "Obtener Certificado". Esta clave pública está en un sitio accesible para todos los empleados del sistema y físicamente es un fichero con extensión .cer y como nombre del fichero el número del empleado.

Una vez seleccionada la clave pública, hay que pulsar el botón de "Cifrar Documento" en la parte inferior del formulario para que la AC cifre el documento con la clave pública del empleado y lo depositará en un repositorio común para todos los empleados. Además hay que firmar dicho contenido del documento, para ello pulsa el botón "Firmar Documento". Esta firma se realiza con la clave privada de la AC y también la depositamos en ese lugar común para los empleados para que pueda comprobar después la veracidad de la firma.

El resultado final de cifrar y firmar documento son los mensajes que aparecen en la parte inferior del formulario, en el lado derecho de los botones. Y lógicamente ha creado un fichero cifrado (con la clave pública del empleado) del documento que se

quiere cifrar con extensión .enc y otro que es la firma de dicho documento que ha realizado la AC con su clave privada y que es un fichero con extensión .frm.

4.4.1.2. Autoridad de Verificación (AV)

Ahora pasamos a describir la interfase de la aplicación relacionada con el usuario AV, este mismo se compone de las siguientes funciones.

1. **AC ⇒ Información Certificado.**
2. **AC ⇒ Consultar CRL.**
3. **AC ⇒ Búsqueda de Certificados Revocados.**

Como en caso 4.4.1.1, en este punto pasamos a analizar en detalles cada uno de los aspectos descritos anteriormente.

1. El primer elemento lo obtenemos al pulsar el botón de **"Información Certificado"** que abre el siguiente formulario:

Figura 4.14: Interfase sobre la Consulta de Estado del Certificado para el usuario AV.

En dicho formulario tenemos que introducir el número de serie del certificado del que queremos obtener la información y pulsar el botón de "buscar certificado". Hay que recordar que cada certificado tiene un único número de serie.

El resultado es la información del certificado que tenemos en la base de datos del sistema, como se muestra en la 4.15.

Figura 4.15: Resultado simulado sobre la consulta del estado del certificado.

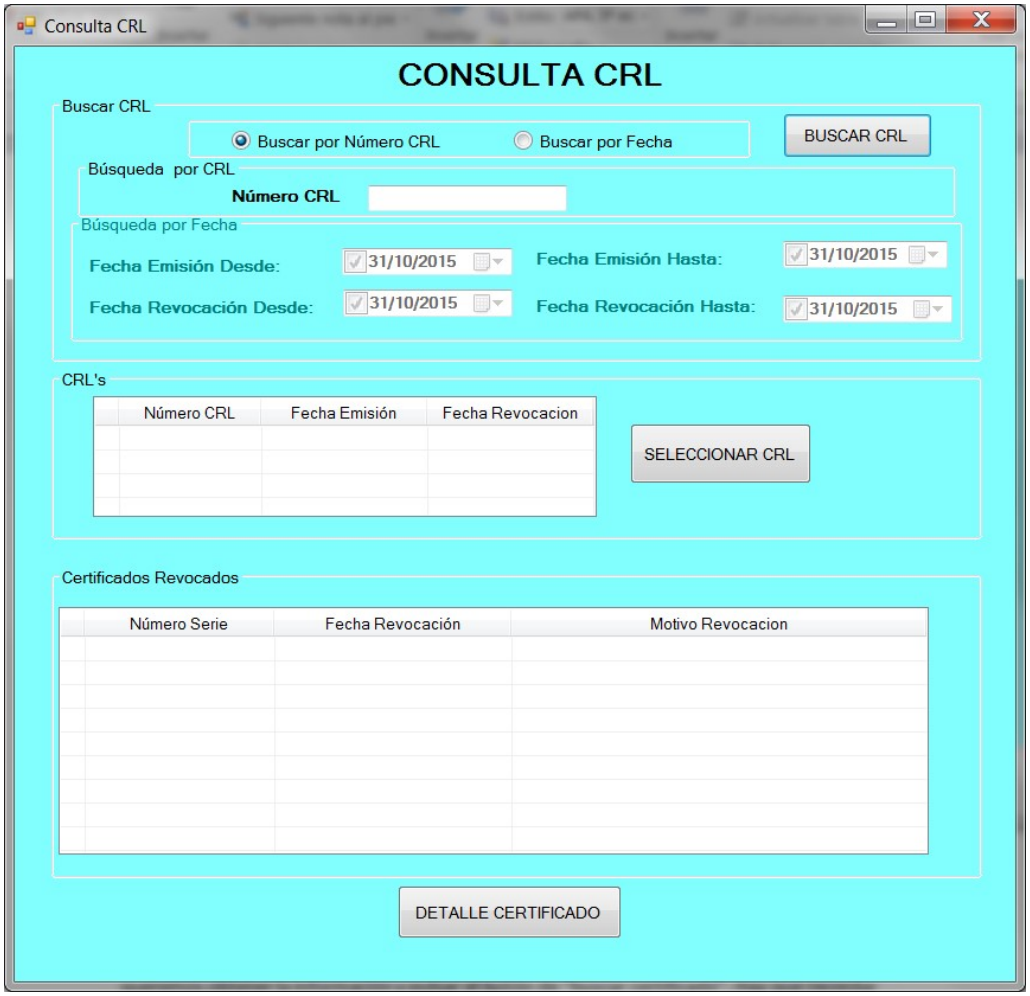


Figura 4.16: Interfase sobre la Consulta CRL.

2. La siguiente función de la parte del usuario AV es la de **"Consultar CRL"**, que sirve para mostrar las listas CRL que hubiera en el sistema así como los certificados revocados que forman parte de cada una ellas. El formulario que se obtiene al pulsar el botón de "Consultar CRL" esta descrito en la Figura 4.16.

   La búsqueda de las CRL las podemos realizar introduciendo directamente el número de la CRL en el campo "Número CRL" o por fecha. En fecha se puede especificar la búsqueda tanto por fecha de emisión como por fecha de revocación. Una vez seleccionados los parámetros de búsqueda pulsamos el botón de "Buscar CRL" situado arriba a la derecha y obtenemos la CRL o CRL's que cumplen con los requisitos de búsqueda.

   Si existen CRL con esos criterios se mostraran en la lista de CRL que está en la parte central del formulario. Si queremos ver los certificados de una de esas listas mostradas tenemos que seleccionar una y pulsar el botón de la derecha con nombre "Seleccionar CRL" y automáticamente nos cargará en la lista inferior todos los certificados revocados de la lista seleccionada, como mostramos en la Figura 4.17.

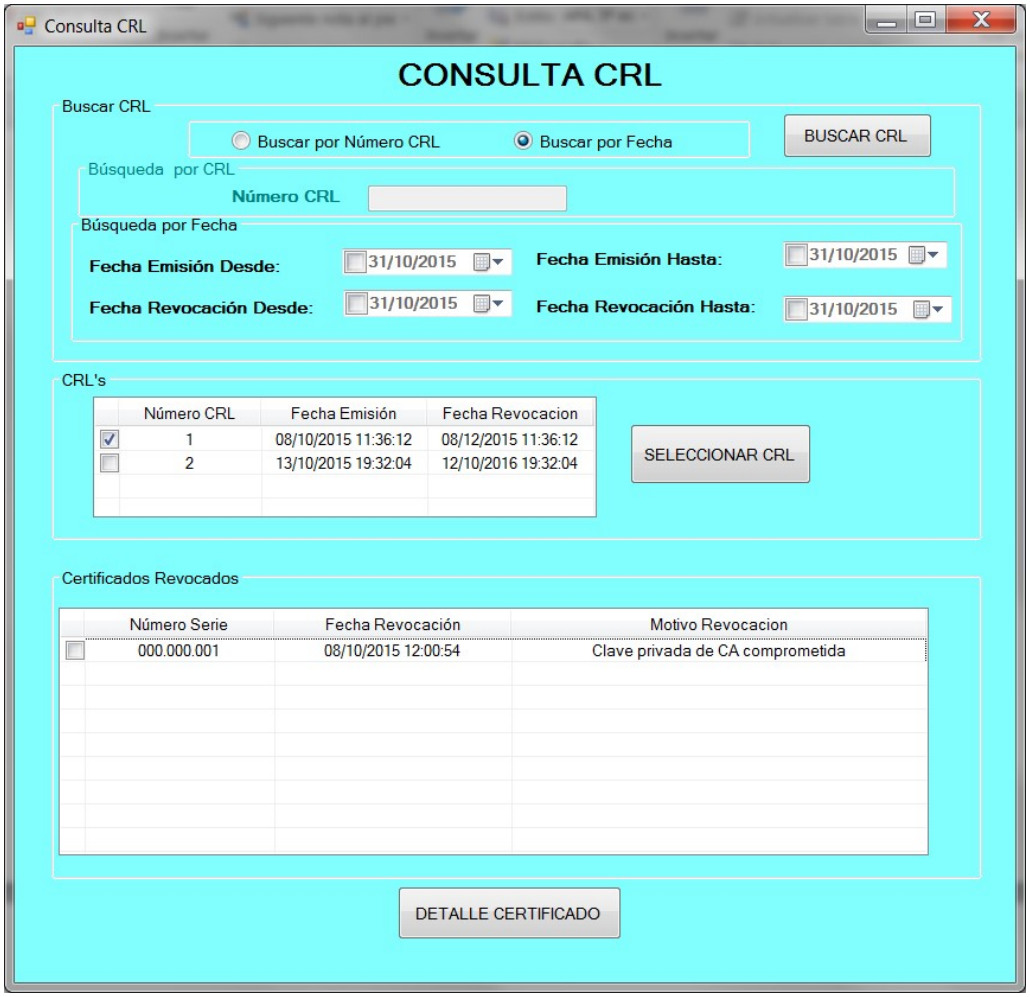


Figura 4.17: Resultado simulado sobre la Consulta CRL.

Y si seleccionamos un certificado en la parte inferior del formulario y pulsamos sobre el botón "Detalle Certificado" nos mostrará información ampliada de dicho certificado, como mostramos en la figura:

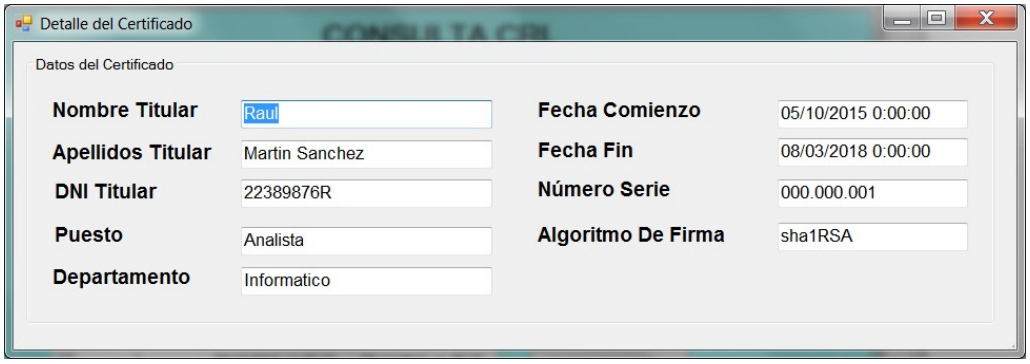


Figura 4.18: Resultado de la Interfase simulada sobre el Detalle de un Certificado.

3. Mediante este formulario se realiza la **"búsqueda de certificados revocados"** que haya en el sistema. Permite buscar los certificados por fecha de revocación de certificados, número de serie del certificado o por el motivo de la revocación. El formulario es como el que se muestra en la Figura 4.19.

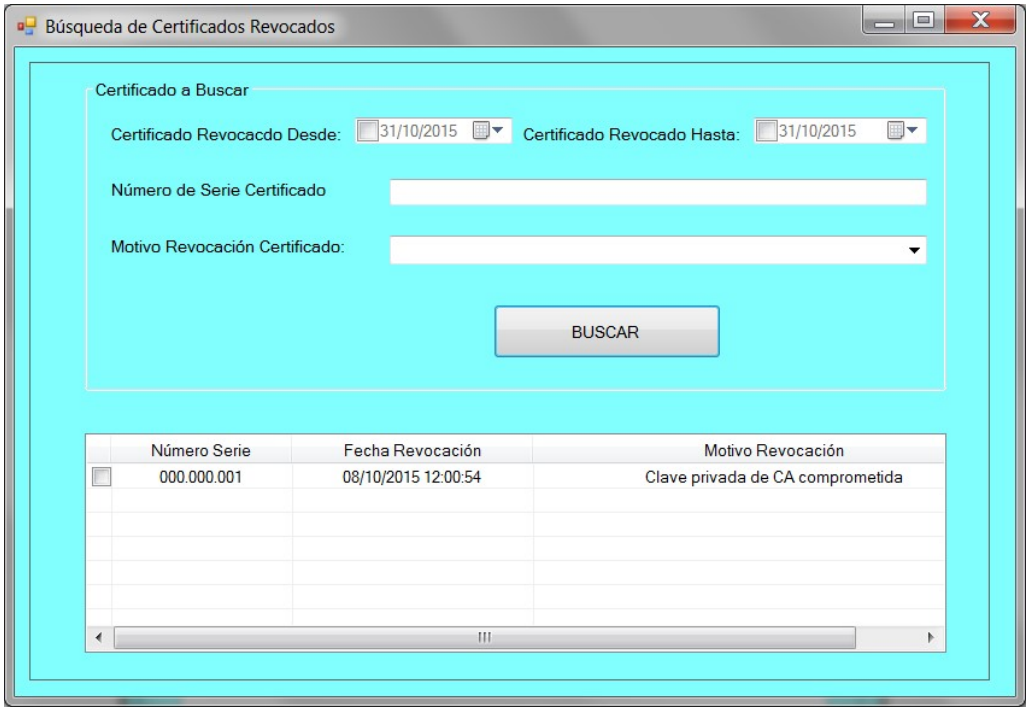


Figura 4.19: Interfase para la Búsqueda de Certificados Revocados.

4.4.1.3. Autoridad de Registro (AR)

Ahora pasamos a describir la interfase de la aplicación relacionada con el usuario AR, este último apartado describe las siguientes funciones de la Autoridad de Registro.

1. **AC ⇒ Gestión Solicitud Certificados.**
2. **AC ⇒ Gestión revocación Certificados.**
3. **AC ⇒ Gestión ciclo vida certificados.**

Como en los casos 4.4.1.1 y 4.4.1.3, en este punto pasamos a analizar en detalles cada uno de los aspectos descritos anteriormente.

1. Pulsando sobre el botón de **"Gestión Solicitud de Certificados"** nos aparecerá el formulario que se encargará de gestionar las solicitudes recibidas de los empleados para la solicitud de creación de certificados. Se puede filtrar la búsqueda por el estado en que se encuentran los certificados o mostrar todos. Una vez mostradas las solicitudes los certificados en la lista central del formulario la AR puede hacer lo siguiente:

   - ***Tramitar Seleccionados*** ⇒ la AR lo que hace es cambiar de estado la solicitud del certificado que está en estado "recibido" y lo cambia al nuevo estado de "En Trámite". Simula el comportamiento de la AR cuando recibe una solicitud de un empleado para solicitar un nuevo certificado.
   - ***Aceptar Seleccionados*** ⇒ la AR simula el proceso de aceptar la solicitud del empleado y dicha solicitud está pendiente a que la AC proceda a crearlo físicamente. Se simula la creación de un certificado con estado "Pre-Activado" y al que se le ha asignado ya su número de serie, pero no el archivo físicamente de dicho certificado.
   - ***Denegar Seleccionados*** ⇒ la AR simula el proceso de denegar o desestimar la solicitud de creación de certificado y queda pendiente de que la AC lo borre físicamente. El estado de la solicitud cambia de "Recibido" a "Denegado".

   El formulario sería como se muestra en la interfase gráfica de la Figura 4.20.

Figura 4.20: Interfase para la Gestión de Solicitudes de Certificados.

2. ulsando sobre el botón de **"Gestión de revocación Certificados"** nos aparecerá el formulario que se encarga de gestionar las solicitudes de revocación de certificados recibidas de los empleados. Como en el caso anterior también se puede filtrar por

el estado en que se encuentran dichas solicitudes de revocación. Una vez mostrados las solicitudes de revocación de certificados en la lista central del formulario la AR puede realizar lo siguiente:

- ***Tramitar Seleccionados*** ⇒ la AR lo que hace es cambiar el estado de la solicitud de revocación de certificado que está en estado "recibido" y lo cambia al nuevo estado de "En Trámite". Simula el comportamiento de la AR cuando recibe una solicitud de un empleado para solicitar una revocación de certificado.
- ***Aceptar Seleccionados*** ⇒ La AR simula el comportamiento de aceptar la revocación que le solicita el empleado y queda a la espera que la AC lo revoque definitivamente. Cambia el estado que tuviera a "Aceptado".

  El formulario sería como el siguiente:

Figura 4.21: Interfase para la Gestión de Solicitudes Revocación de Certificados.

3. Pulsando sobre el botón de **"Gestión ciclo vida certificado"** nos aparecerá un formulario que muestra el ciclo de vida de un certificado del sistema. Indicando por todos los estados por lo que ha pasado, desde que se solicita, hasta que es finalmente revocado.

   Para realizar la búsqueda del certificado lo podemos hacer por el número de serie de dicho certificado o bien por el DNI del empleado, ya que un empleado del sistema sólo puede tener un certificado. También muestra la información del titular del certificado.

   El formulario sería como se muestra en la interfase gráfica de la Figura 4.22

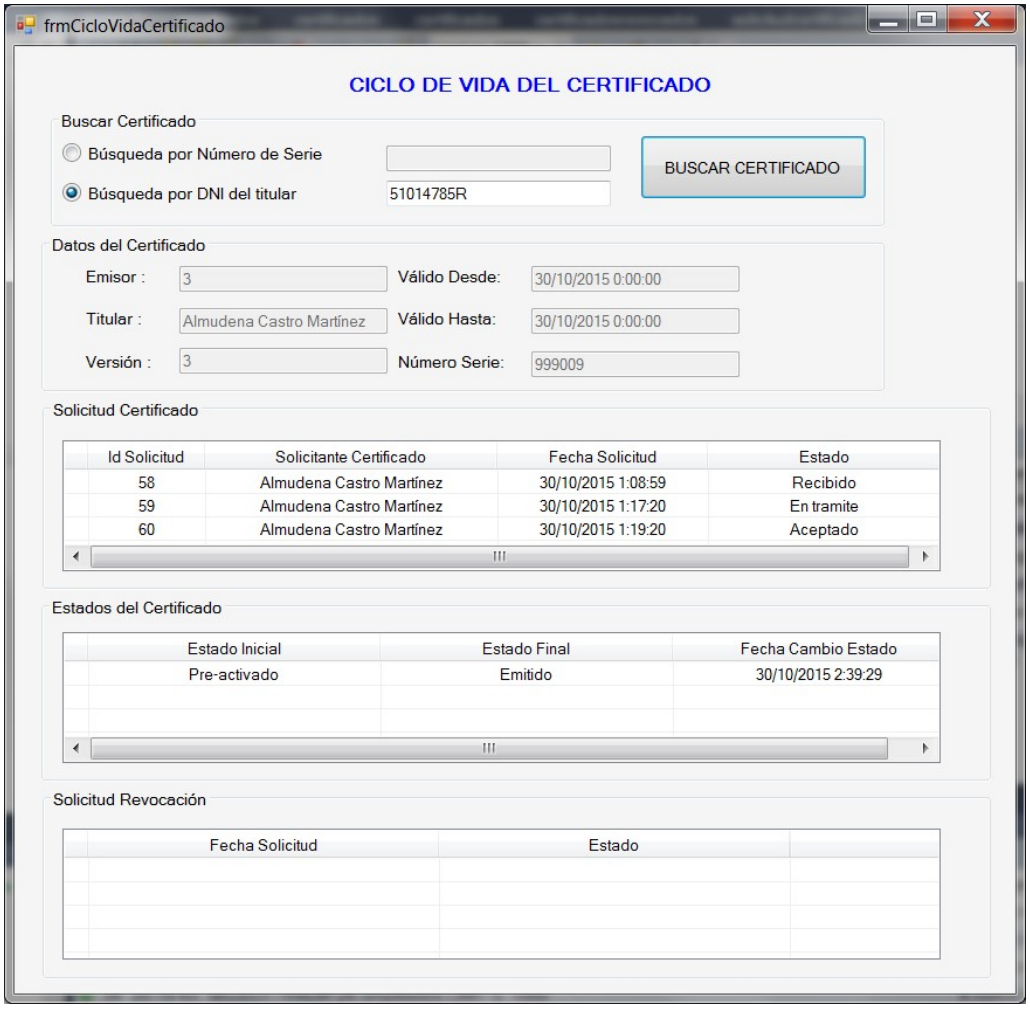


Figura 4.22: Interfase para la Gestión de Búsqueda de un Certificado.

4.4.2. Interfase de la Aplicación desde la perspectiva de un Empleado

En este apartado al igual que en el anterior 4.4.1 intentaremos describir de forma general los principales aspectos que la interfase gráfica de la aplicación creada presenta para un usuario Empleado. Como es de esperar las funcionalidades de este módulo de la aplicación es diferente al anterior 4.4.1 por lo que se hace necesario una breve descripción de la interacción del empleado con la aplicación. Sin nada más, pasamos a describir los pricipales formularios de interacción, primeramente enumerándolos cada uno de ellos en la siguiente lista de funcionalidades:

1. **Solicitar Certificado.**
2. **Solicitar Revocar Certificado.**
3. **Visualizar documentos cifrados.**
4. **Envío de documentos cifrados y firmados.**

1. Pasamos a explicar la primera opción. Pulsamos el botón de **Solicitar Certificado** y nos aparecerá el formulario en el que un empleado solicita la creación de un certificado y se lo envía a la AR. Para ello tendrá que introducir el DNI del empleado nos cargará los datos del cliente, siempre y cuando no tenga ya un certificado ya que en ese caso

mostrará un mensaje como el siguiente indicando que no se puede realizar dicha acción y deshabilitará el botón de "Enviar solicitud" que es el que se encarga de realizar la solicitud.

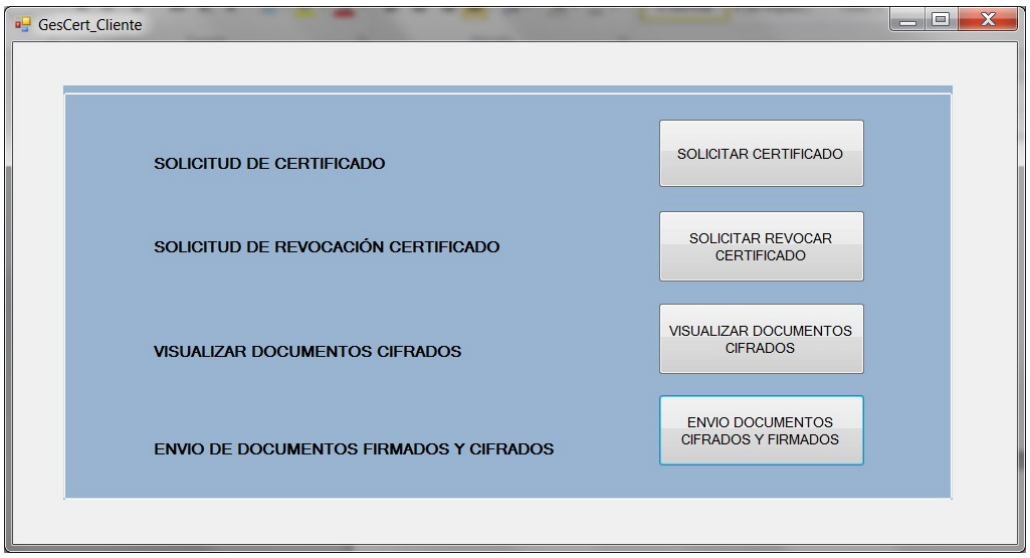


Figura 4.23: Interfase prinicipal para la Gestión de un Empleado.

Figura 4.24: Resultado simulado sobre la duplicidad de un certificado.

Al pinchar la primera opción **"solicitar certificado"** se mostrará una interfase en la cual se pide los datos del empleado tal y como se muestra en el formulario de la figura 4.25.

Figura 4.25: Interfase para la Gestión de Búsqueda de un Certificado.

Una vez cargados los datos del empleado que solicita el certificado, solo tiene que seleccionar la fecha de solicitud y pulsar el botón "Enviar Solicitud". Dicha solicitud le llegará a la AR para gestionar la solicitud de empleado.

2. **Solicitar Revocar Certificado**, es donde el empleado realiza la revocación de su certificado digital para comunicárselo a la AR. Esta revocación puede ser por múltiples motivos pero normalmente es porque se ha comprometido la clave privada del empleado.

Para ello el empleado debe introducir su DNI o número de serie del certificado que quiere revocar y el sistema verificará que el empleado tiene ya un certificado generado. En caso de que el empleado no tuviera un certificado creado mostraría un mensaje de error indicando esto.

Figura 4.26: Interfase para la Solicitud de Revocación de un Certificado.

El empleado tendrá simplemente que seleccionar el motivo de la revocación de certificados y pulsar el botón "solicitar revocación". Entonces se emitirá dicha solicitud para que lo analice la AR.

3. **Visualizar documentos cifrados** es el formulario que realiza la visualización de documentos cifrados previamente por la AC con la clave pública del empleado al que va dirigido. Y que el empleado al poseer en su equipo su clave privada (en este caso contenida en el certificado .pfx) podrá descifrar dicho contenido. El archivo .pfx al crearse inicialmente por la AC permite elegir una contraseña para aumentar la seguridad del proceso, nosotros para simplificar el proceso hemos optado por dejarlo en blanco, por lo que el fichero .pfx no requiere introducir ninguna contraseña adicional. El empleado tendrá que tener instalado en su equipo dicho certificado (con la clave privada) para que el sistema pueda descifrarlo y abrir el contenido.

   Como hemos mencionado anteriormente, los nombres de los documentos cifrados en el sistema tienen un formato determinado, mediante el cual nos permite saber solo con dicho nombre a qué empleado va
   dirigido dicho contenido.

   Por lo que el empleado debe introducir el nombre del documento a descifrar en la parte superior del formulario, y el sistema cargará los datos del empleado debajo de la ruta que ha introducido donde buscar el fichero. El sistema también intentará descifrar el documento con la clave privada del empleado que deberá tener instalada en el su equipo mediante el certificado .pfx. Si todo esta correcto lo descifrará y mostrará un mensaje por pantalla un mensaje como se muestra en la interfase gráfica de la Figura 4.27.

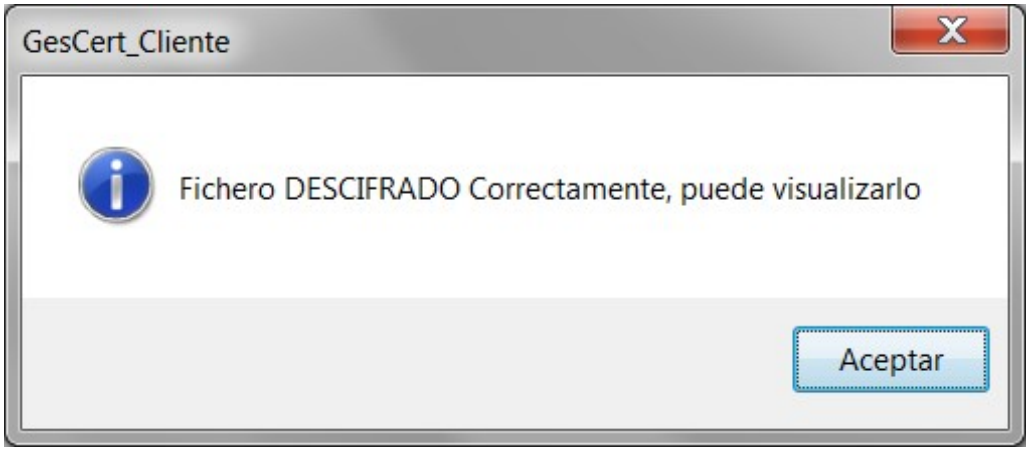


Figura 4.27: Interfase simulada para el correcto descifrado de un Documento.

Entonces el empleado podrá visualizar el contenido del documento pulsando el botón que se ha habilitado al concluir satisfactoriamente y que ejecutará Adobe Acrobat para abrir el documento descifrado.

El formulario que realiza todo este proceso está descrito en la Figura 4.28:

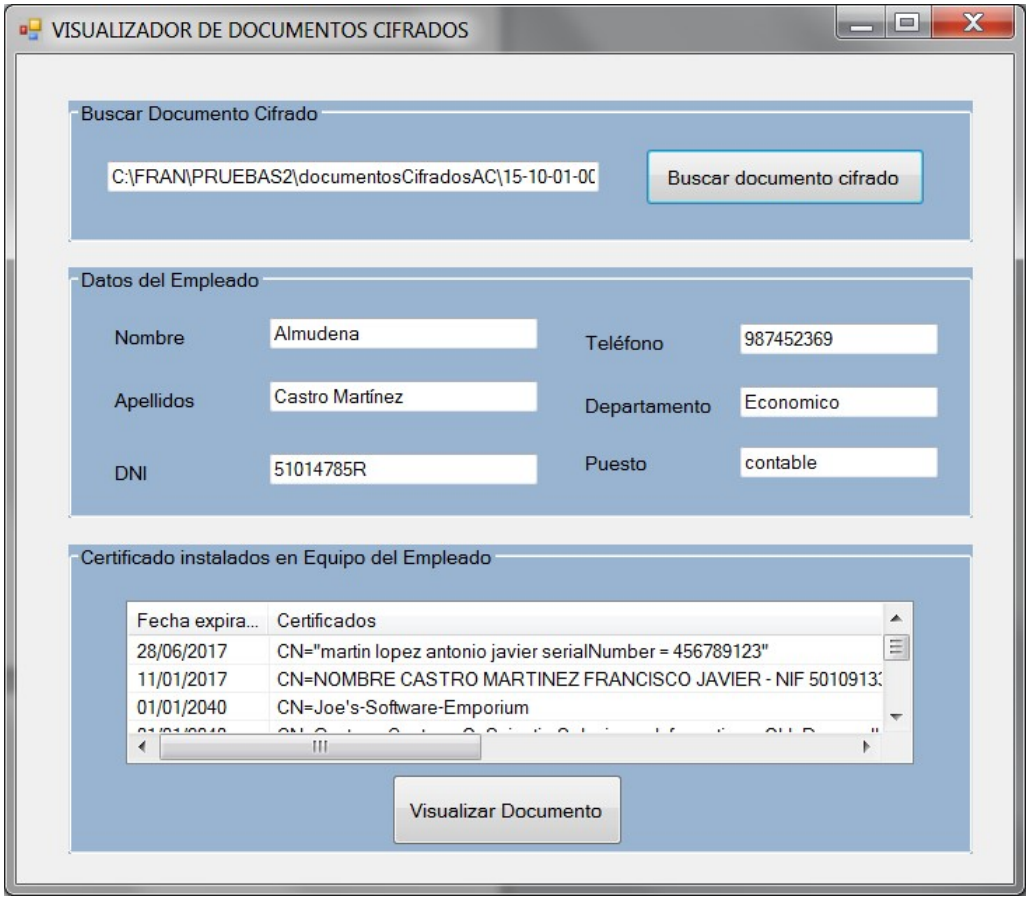


Figura 4.28: Interfase para la Gestión de Búsqueda de un Documento Cifrado.

Nota: en el formulario se muestran también otros formularios que tuviera instalados en su equipo el empleado.

4. **Envío de documentos cifrados y firmados**esta parte de la aplicación es donde los empleados realizan el cifrado, descifrado, firma y verificación de firma de documentos entre ellos. El formulario seria como se muestra en la interfase gráfica de la Figura 4.29.

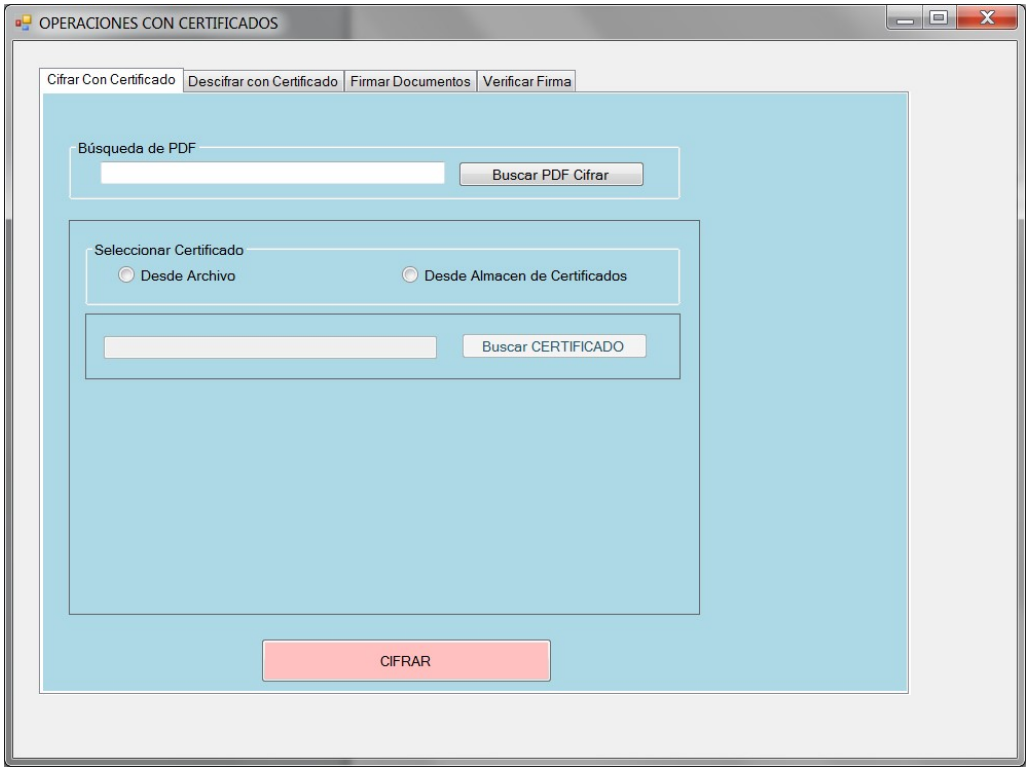


Figura 4.29: Interfase para las Operaciones con Certificados.

Donde se puede apreciar en la parte superior una serie de pestañas para realizar las siguientes acciones:

- ***Cifrar con certificado*** ⇒ Esta pantalla sirve para cifrar un documento de un empleado emisor a otro empleado receptor. El empleado A que quiere enviar un documento a otro empleado B lo primero que tiene que hacer es buscar el documento que quiere enviar pulsando el botón "buscar PDF cifrar" en la parte superior y a continuación el empleado A tendrá que buscar la clave pública del empleado B al que se lo quiere enviar. Esto lo puede hacer buscando directamente el certificado en la ubicación donde están todos las claves públicas de los empleados del sistema (marcando "desde archivo") o bien en el caso que tuviera la clave pública del empleado en el almacén de certificados de la máquina del empleado A (la opción "desde almacén de certificados y a continuación seleccionarlo de la lista que aparecen). Una vez seleccionado la clave pública del empleado B, el empleado A pulsará el botón situado en la parte inferior del formulario "Cifrar" y el sistema realizará el cifrado del documento con la clave pública de B utilizando el fichero con extensión .cer (certificado con nombre xxxxxx.cer, siendo x el número del empleado). Al realizar el cifrado tiene que verificar previamente el sistema que dicho certificado no este revocado y que tampoco este expirado.

  El resultado de dicho cifrado es un fichero con nombre igual al documento original con una extensión .enc y situado en un lugar común para todos los empleados del sistema y que viene parametrizado en un fichero .INI en la aplicación.

- Seleccionando en la pestaña superior la opción ***Descifrar con certificado*** ⇒ nos aparecerá un formulario como se muestra en la interfase gráfica de la Figura 4.30.

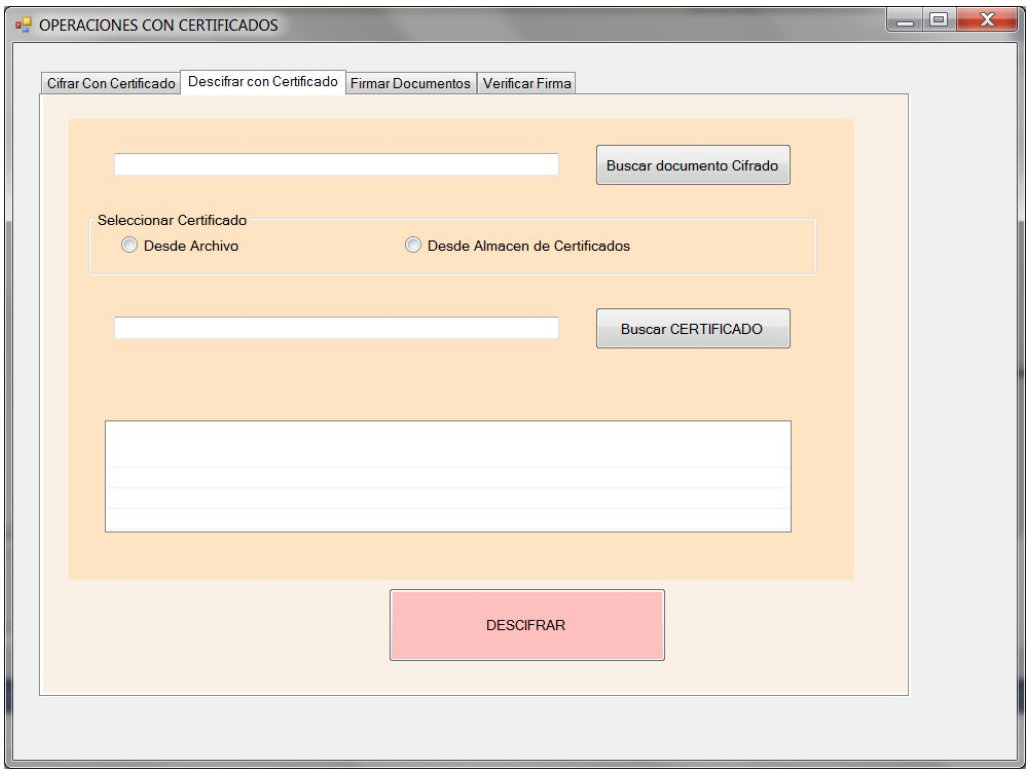


Figura 4.30: Interfase simulada para cargar un Documento previamente cifrado.

Este formulario realiza la función inversa a la del punto 4, es decir, se encarga de descifrar un documento previamente cifrado.

El proceso se realiza de la siguiente manera: el empleado A, que quiere descifrar un documento que previamente lo ha cifrado otro empleado B, tiene que seleccionar el documento cifrado pulsando el botón de la parte superior derecha del formulario, "buscar documento cifrado", este archivo tiene una extensión .enc y como nombre del fichero el número del empleado A. Este documento cifrado por B se hizo cifrándolo con la clave pública de A y ahora el empleado A tiene que utilizar su clave privada para poder descifrarlo. (El proceso es similar a la opción explicada anteriormente para "visualizar documentos cifrado" y abierto con Adobe Acrobat). Para utilizar su clave privada, el empleado A tiene que seleccionarla o bien desde una ubicación especifica donde este dicho certificado (con extensión .pfx) o bien desde su propio equipo en el almacén de certificados, como se muestra en la interfase gráfica de la Figura 4.20.

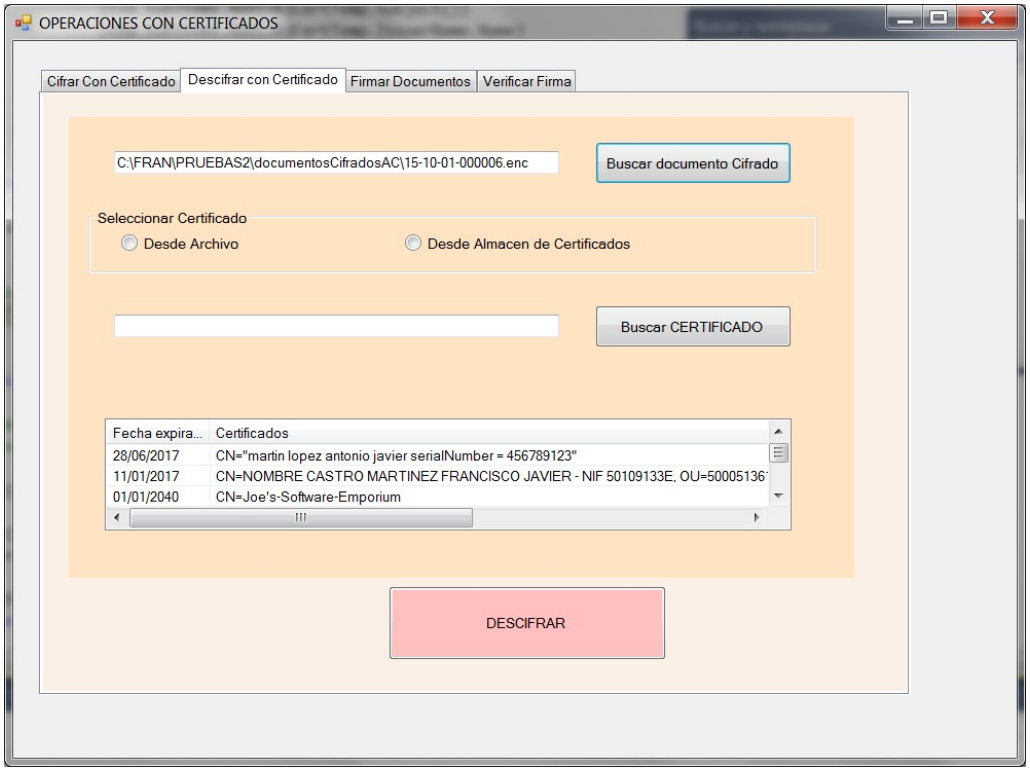


Figura 4.31: Respuesta simulada sobre el descifrado de un documento.

Una vez seleccionada la clave privada del empleado A (desde ubicación o desde el almacén de certificados) pulsará el botón en la parte inferior del formulario y el sistema procederá a descifrar el documento.

El resultado de descifrar el documento cifrado (con extensión .enc) es el mismo nombre del fichero con extensión .pdf, en una ubicación que tienen parametrizados los empleados en el fichero .INI de la aplicación.

- Si seleccionamos la pestaña ***Firmar Documentos*** $\Rightarrow$ nos aparecerá el siguiente formulario como se muestra en la interfase gráfica de la Figura 4.20.

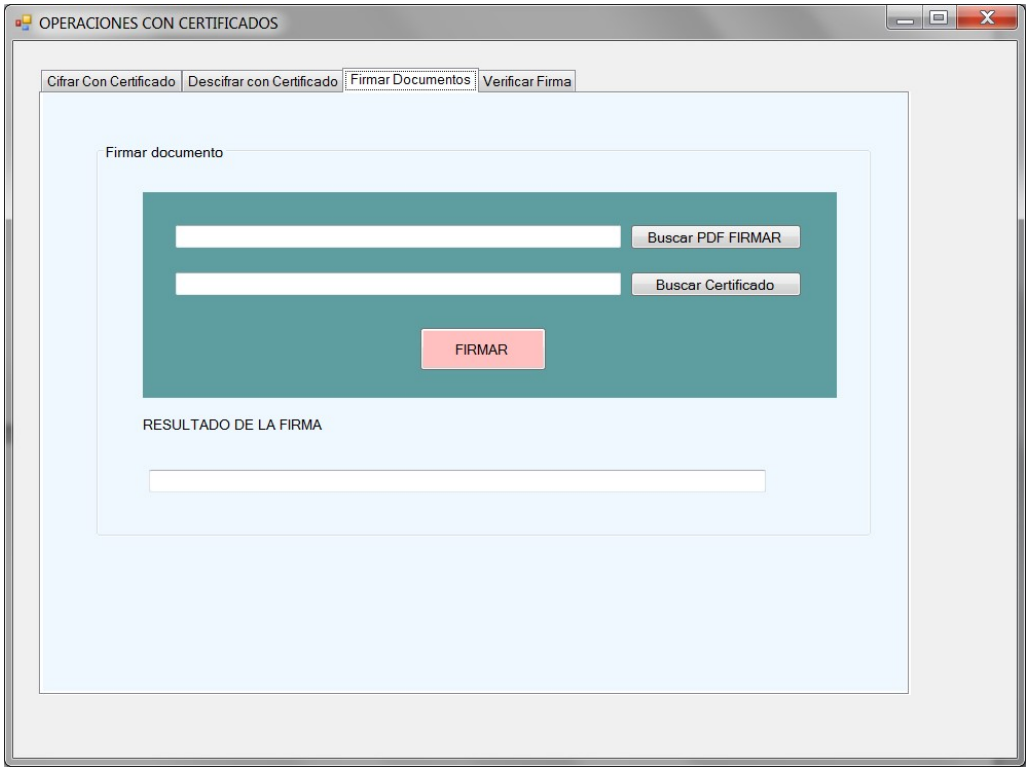


Figura 4.32: Interfase para la Gestión de Firmar un Documento.

Este formulario realiza la firma de un documento del sistema. Para firmar un documento el empleado selecciona el documento que quiere firmar pulsando el botón de la parte superior derecha "Buscar PDF Firmar" y a continuación pulsar el botón "Buscar Certificado" para buscar el certificado del empleado que contiene la clave privada del empleado con la que firmará el documento. (Este certificado tendrá la extensión .pfx).

Para firmar el documento lo que hace es aplicar una función resumen o hash a dicho documento y a continuación cifrarlo con la clave privada del empleado. El resultado es un fichero con extensión .frm. Y que se puede utilizar en conjunto con la pestaña anterior de "Cifrar con Certificado" para enviar el documento cifrado y la firma a otro empleado.

- Si seleccionamos la pestaña ***Verificar Firma*** $\Rightarrow$ nos aparecerá el siguiente formulario como se muestra en la interfase gráfica de la Figura 4.33.

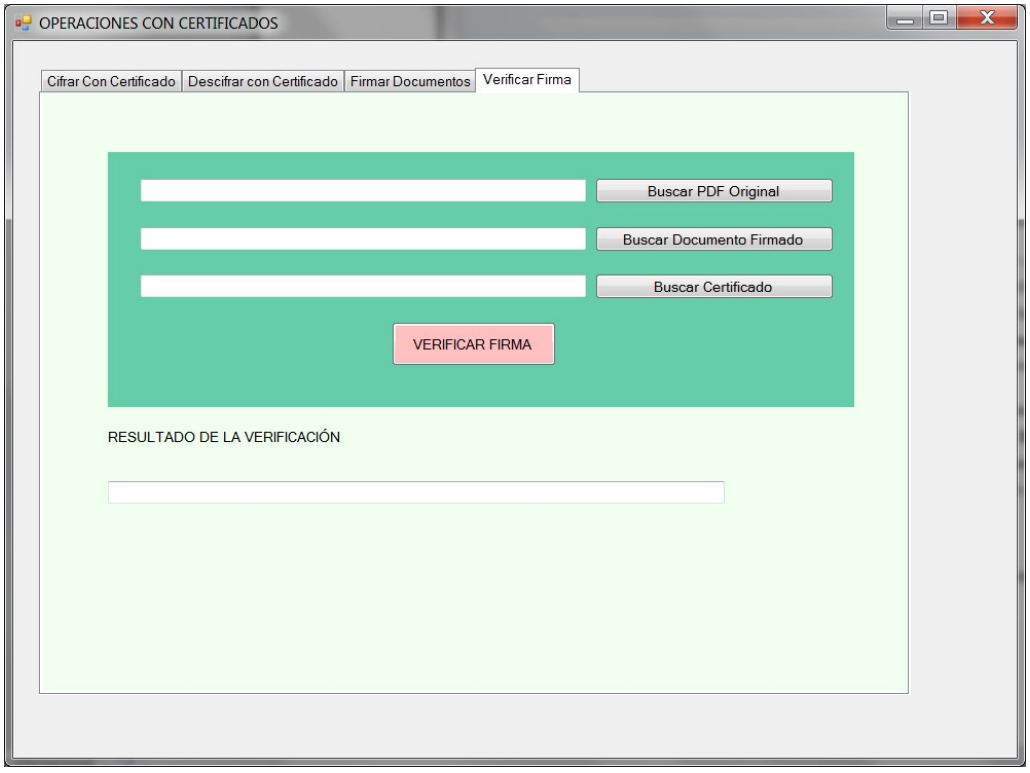


Figura 4.33: Interfase para la verificación de la Firma.

Que es el formulario que sirve para verificar una firma de un documento previamente firmada por un empleado. El proceso sería el siguiente:

a) El empleado A que quiere verificar el contenido de una firma pulsa en el formulario el botón "Buscar PDF original" que es el documento original que se ha firmado.

b) El empleado A selecciona el documento firmado que le ha enviado o que ha firmado un empleado B pulsando el botón "Buscar Documento Firmado". Dicho documento tiene extensión .frm.

c) El empleado A selecciona la clave pública del empleado B pulsando el botón "buscar certificado" (certificado con extensión .cer)

d) Con estos tres elementos el sistema descifra la firma que ha creado el empleado B y que ha seleccionado en el paso anterior utilizando la clave pública del empleado B.

e) A continuación el sistema genera su propio hash con el documento original y lo compara con el valor obtenido en (4), si ambos valores coinciden la verificación de la firma es correcta, en caso contrario el documento se ha modificado o no es el mismo con el que se firmó el documento.

Capítulo 5

Conclusiones y Trabajo Futuro

Una vez concluidas todas las fases del proyecto procedemos a mencionar las conclusiones obtenidas de la realización, así como las líneas o trabajo futuro que se puede realizar ampliando y mejorando lo realizado hasta ahora.

5.1. Conclusiones

A continuación exponemos las conclusiones más relevantes como consecuencia de la realización del proyecto fin de carrera.

5.1.1. Aportaciones

En primer lugar se puede concluir que la misión u objetivo principal del proyecto se ha conseguido, y que no es otra, que realizar una gestión de certificados para una pequeña empresa e implementar para ello una PKI. Y todo ellos explicarlo desde un punto de vista didáctico y abarcando los diferentes método criptográficos que se disponen actualmente, empezando por los más sencillos y acabando con los más complejos. Con esto queríamos ver cómo aplicar estos métodos teóricos a un caso práctico y ver cómo se puede integrar todo y conseguir que la os documentos que la empresa quiera proteger se les garantice la integridad, no repudio, confidencialidad y autenticidad.

Muchas empresas se "conforman" con poner una contraseña al documento que quieren proteger, si bien esto puede ser suficiente dependiendo de qué entornos, nosotros proponemos un sistema mucho más completo y seguro. Todo ello gracias a los certificados digitales.

Estos certificados son creados por la propia empresa que implementa el sistema PKI por lo que pueden personalizarlo a sus necesidades y que todos los empleados de dicha empresa lo utilicen para tener una documentación confidencial mucho más segura. Estos certificados generados son totalmente válidos y se podrían utilizar en otras aplicaciones que los utilizaran, si bien es cierto, que una de las partes más importantes de los certificados es la confianza de la Autoridad de certificación que lo emite, y si por tanto esta no es confiable, dicho certificado tiene poca utilidad. Pero en teoría se podría utilizar. Por eso este sistema es más local, ya que el que otra empresa o entidad confié en nosotros tiene que ser gracias a la AC y éstas suelen ser pocas y muy grandes, para garantizar esa confianza y sobre todo la relación entre una identidad de una persona y su clave pública.

5.1.2. Dificultades del proyecto

El realizar un trabajo de estas características desde cero y realizando todas las fases de análisis, desarrollo e implementación implica ya de por si una dificultad añadida. Así como el documentar y buscar una gran cantidad de información para poder abordar el proyecto. Como dificultades encontradas en el proyecto fueron principalmente ver en qué consiste un certificado digital, como crearlo, realizar con él las operaciones de cifrado, descifrado, firma y verificación de firma, y ver como gestiona Windows los certificados una vez creados. Además teníamos que ver cómo trabaja una PKI, qué componentes tiene, cómo crear nuestra PKI y adaptarlo con el modelo de empresa a la que queríamos integrarlo. El crear físicamente los certificados también nos llevó bastante tiempo primero por ver las herramientas que existen, que son muy pocas, y después configurarla correctamente para poder crearlos

5.1.3. Conclusiones personales

Como conclusión personal tengo que mencionar una dificultad añadida a la realización del proyecto y que ha sido el tener que compaginarlo con una jornada laboral completa y a una gran distancia de mi domicilio, de ahí que encontrar el tiempo necesario para realizar dicho proyecto haya supuesto un esfuerzo añadido, ya que muchas veces no tenías esas energías o motivación para ponerte a realizarlo. Pero a pesar de eso, el poder finalizarlo supone una gran satisfacción y vale la pena pasar por ello.

El utilizar tecnologías con las que no estás familiarizado ni trabajas habitualmente también supone una dificultad, y el tener que dedicarle mayor tiempo para comprenderlas hace que el proyecto fuera un poquito más lento.

Pero como el área de seguridad siempre ha sido en la carrera una de las asignaturas que más me gustaban, la realización del proyecto también ha sido más llevadera, sobre todo por las cosas que vas aprendiendo y que ves que tienen múltiples aplicaciones en la vida real y todo lo que hay aún por hacer...

5.2. Trabajo Futuro

Como trabajo futuro habría que comentar en primer lugar que la PKI que hemos implementado es con sus componentes básicos y que por tanto se pueden ampliar para hacerla más completa.

Una de las cosas que habría que modificar sería el lugar donde se depositan los certificados. Nosotros simplemente los hemos dejado en una carpeta donde tengan acceso todos los empleados de la empresa, ya que se trata de certificados con la clave pública de cada empleado, y son necesarios para poder cifrar documentos entre los empleados y los que genera la AC. Deberíamos utilizar LDAP (Light-weight Directory Access Protocol) para acceder a los directorios. Puesto que LDAP soporta la Capa de conexión segura (SSL) y la Seguridad de la capa de transporte (TLS), los datos confidenciales se pueden proteger de personas no autorizadas.

Al implementar dicha LDAP las listas de revocación de certificados también habría tendría que descargarla de ahí el empleado que quisiera acceder a dicho contenido. El sistema lo hace mediante un formulario Windows que de conecta a la base de datos para obtener

la información de las listas de certificados revocados (CRL) junto con los certificados revocados que tuviera cada una.

Nosotros hemos implementado para suministrar la información del estado de un certificado un formulario que se conecta a la base de datos y nos devuelve dicha información. En teoría habría que implementar un protocolo OCSP (Online Certification Status Protocol) para realizar dicha tarea, si bien seguiría siendo la AC la que actualiza dicha información.

También sería necesario si queremos darle mayor seguridad el tener un servicio de backup y archivo seguro de claves de cifrado.

Si queremos añadir más seguridad al sistema y por tanto más complejidad podemos optar por implementar también otro componente opcional de la PKI que es la Autoridad de Sellado de Tiempos (TSA), que permite firmar documentos con sellos de tiempos, de manera que permite garantizar que un determinado documento existía en una fecha concreta.

Otra posible mejora que se podría realizar sería el implementar el certificado en una tarjeta criptográfica en lugar de tener los ficheros de los certificados físicamente.

Pero también se podrían definir todos los aspectos legales, de protocolos y procedimientos que también forman parte del funcionamiento de la PKI y que estos se escapaban del alcance del proyecto. Estos serían por ejemplo las políticas de seguridad, para definir las reglas bajo las cuales deben operar los sistemas criptográficos. Además los procedimientos que especifican cómo generarse, distribuirse y utilizarse las claves y certificados. Muy importante también establecer la política de certificación y la declaración de prácticas de certificación (CPS), que indica cuales son las practicas utilizadas para emitir los certificados. Incluye los equipos, las políticas y procedimientos a implantar para satisfacer las especificaciones de la política de certificación. Se trata de un documento publicable.

Como se puede observar el implementar una PKI completa y con todos sus elementos es una tarea muy compleja y desde el punto de vista de futuras líneas de ampliación hay mucho trabajo que se puede ampliar...

Acrónimos

Bibliografía

[1] BOE.
Titulo II, Capítulo I, Ley 59/2003, de 19 de diciembre, de firma electrónica.
http://www.boe.es/diario_boe/txt.php?id=BOE-A-2003-23399, 2015.
[Online; accedido 21-September-2015].

[2] Dave Cooper.
Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile.
tools.ietf.org, 2008.
[Online; accedido 29-September-2015].

[3] Roberto Gómez Cárdenas.
Certificados Digitales y PKI.
http://homepage.cem.itesm.mx/rogomez, 2014.
[Online; accedido 19-September-2015].

[4] PDF Creator.
The Free PDF Converter Tool.
http://www.pdfforge.org/pdfcreator, 2015.
[Online; accedido 19-September-2015].

[5] Universidad Politécnica de Valencia.
¿Qué es un certificado digital?
http://www.upv.es/contenidos/CD/info/711545normalc.html, 2015.
[Online; accedido 22-September-2015].

[6] DigiSigner.
DigiSigner: Free Electronic Signature Service.
https://www.digisigner.com/, 2015.
[Online; accedido 24-September-2015].

[7] EcoFirma.
Virtual Office.
https://oficinavirtual.mityc.es/javawebstart/soc_info/ecofirma/index.html, 2015.
[Online; accedido 20-September-2015].

[8] eCoFirma organization.
Aplicación eCoFirma 1.4- Utilidad de Copia, Firma y Validación electrónica.
https://oficinavirtual.mityc.es/javawebstart/soc_info/ecofirma/index.html, 2015.
[Online; accedido 20-September-2015].

[9] Portal Administración electrónica de España.
@FirmaFacil.

http://firmaelectronica.gob.es/Home/Empresas/Aplicaciones-Firma.html, 2015.
[Online; accedido 20-September-2015].

[10] Portal Administración electrónica de España.
Plataforma de validación de firma electrónica @firma@Firma.
http://administracionelectronica.gob.es/ctt/afirma#.VYHYsc-8PGc, 2015.
[Online; accedido 20-September-2015].

[11] eprinsa.
Firmador de Escritorio.
http://www.eprinsa.es/firmador/, 2015.
[Online; accedido 28-September-2015].

[12] Jalal Feghhi, Jalil Feghhi, and Peter Williams.
Digital certificates.
Addison Wesley, 1999.

[13] Aránzazu García Hermo.
La facturación electrónica como herramienta para la mejora de la eficiencia en los procesos y el intercambio electrónico de información en el sector de automoción.
e-archivo.uc3m.es, 2012.

[14] iSafePDF.
The open source PDF protection software.
http://isafepdf.eurekaa.org/, 2015.
[Online; accedido 27-September-2015].

[15] Ignacio Jiménez Pinto.
Sistema de autenticación global en una red empresarial.
E_ Informatica, 2014.

[16] Jordi Herrera Joancomartí, Joaquín Garciía Alfaro, and Xavier Perramón Tornil.
Aspectos avanzados de seguridad en redes.
UOC Formación de Posgrado, 2004.

[17] JSignPdf.
JSignPdf.
http://jsignpdf.sourceforge.net/, 2015.
[Online; accedido 13-September-2015].

[18] LibreOffice.
Open Office.
https://es.libreoffice.org/, 2015.
[Online; accedido 20-September-2015].

[19] Francisco Ronaldo Medina Huerta et al.
Desarrollo en python de una plataforma para la revocación de certificados digitales en vanets.
Universitat Politčcnica de Catalunya, 2010.

[20] VALIDe organization.
VALIDe.
http://administracionelectronica.gob.es/ctt/valide#.VYZ_xfntnyA, 2015.
[Online; accedido 20-September-2015].

[21] PortableSigner.
A Commandline and GUI Tool to digital sign PDF files with X.509 certificates.

https://github.com/pflaeging/PortableSigner2, 2015.
[Online; accedido 20-September-2015].

[22] PortalDNIe.
DNI Electrónico, Cuerpo Nacional de Policía. Conceptos Básicos.
http://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1001&id_menu=%5B50%5D, 2015.
[Online; accedido 23-September-2015].

[23] José Fabián Roa Buendía.
Seguridad Informática. ISSN: 1696-8352.
McGraw-Hill, España, 2013.

[24] Sergio Sánchez García.
Solución para la delegación de identidad en Sistemas de Gestión de Identidad paneuropeos basada en infraestructuras de certificación y lenguajes formales de asertos de seguridad.
PhD thesis, E_Telecomunicacion, 2010.

[25] Jordi Serra Serra.
Gestión de los documentos digitales: estrategias para su conservación.
Profesional de la Informacion, 2001, vol. 10, núm. 9, p. 4-18, 2001.
Publicado por: EPI-El Profesional de la información.

[26] PDF Sign.
Command line PDF signature tool.
http://pdfsign.codeplex.com/, 2015.
[Online; accedido 20-September-2015].

[27] Sinadura.
La firma digital libr.
http://www.sinadura.net/es/, 2015.
[Online; accedido 25-September-2015].

[28] Francisco Javier Sánchez Herrera and Juan Carlos Román Cortes.
Firma electrónica. esquema de identificación y firma en la aeat.
Unidad de Seguridad Informática. Departamento de Informática Tributaria, 2014.

[29] Sergio Talens-Oliag.
Introducción a los certificados digitales.
https://people.debian.org/~sto/articulos_bei/BEI-2003-11/certificados_digitales.pdf, 2015.
[Online; accedido 22-September-2015].

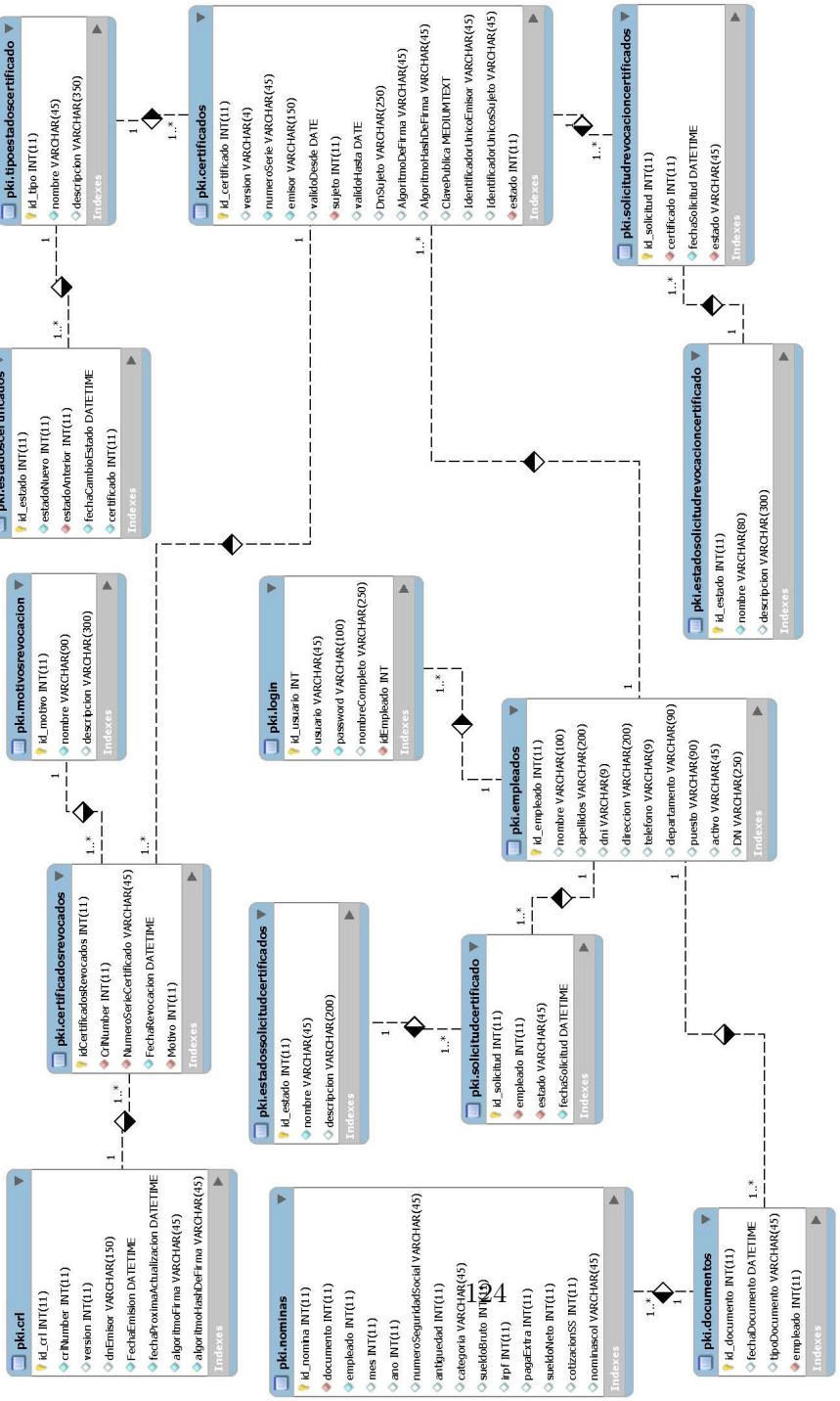
[30] Diana Carolina Valbuena Pabón and Edgar Hernán López Cárdenas.
Modelo de gestión de servicios pki basado en una arquitectura orientada a servicios.
Pontificia Universidad Javeriana, Bogotá, Colombia, 2006.

[31] XolidoSign.
XolidoSign.
http://www.xolido.com/lang/, 2015.
[Online; accedido 26-September-2015].

Apéndices

Apéndice A

Modelo de Datos



Apéndice B

Gestión de Proyecto

B.0.1. Planificación del Trabajo

En esta sección se muestra la planificación inicial y el real del proyecto, así como un pequeño análisis de la desviación entre ambas planificaciones y su justificación.

Para el proceso de desarrollo se ha seguido el modelo en cascada, en el cual al finalizar cada una de las fases se ha llevado a cabo una revisión para determinar si continua con la siguiente fase o por el contrario es necesario realizar algún cambio en alguna de las fases anteriores.

B.0.2. Planificación Inicial

En esta sección mostramos la planificación inicial, dividida en las fases en las que se compone el desarrollo. En cada una de estas fases se ha indicado el tiempo estimado para que se lleven a cabo, expresado en horas.

La planificación inicial consta de 724 horas, distribuidas entre el 23/03/2015 y el 22/09/2015. Hay que señalar que la jornada de trabajo en días laborables es de 3 horas diarias de 19:30 a 22:30 debido a que tenemos que compaginarlo con una jornada laboral completa y sumarle el tiempo de desplazamiento al trabajo en dicha jornada laboral. Y para los fines de semana y festivos un horario de trabajo de 8 horas, lo que significa que el número de horas semanales trabajadas ascienda a 31.

Tabla B.1: Planificación inicial del proyecto.

Nombre	Horas	Fecha Inicio	Fecha Fin
Proyecto	724	23/03/2015	22/09/2015
Planificación	10	23/03/2015	26/03/2015
Estado del Arte	120	26/03/2015	26/04/2015
Análisis	130	26/04/2015	26/05/2015
Planteamiento del problema	6	26/04/2015	27/04/2015
Perspectiva de la solución	20	28/04/2015	02/05/2015
Estudio tecnológico	25	03/05/2015	09/05/2015
Definición de la arquitectura preliminar	24	09/05/2015	14/05/2015
Definición de casos de uso	30	14/05/2015	21/05/2015
Análisis de requisitos	25	22/05/2015	26/05/2015
Diseño	74	27/05/2015	13/06/2015
Elaboración del modelo de datos	35	27/05/2015	05/06/2015
Definición de interfaces de usuario	30	05/06/2015	11/06/2015
Arquitectura definitiva	9	12/06/2015	13/06/2015
Implementación	350	13/06/2015	13/09/2015
Pruebas	40	13/09/2015	22/09/2015

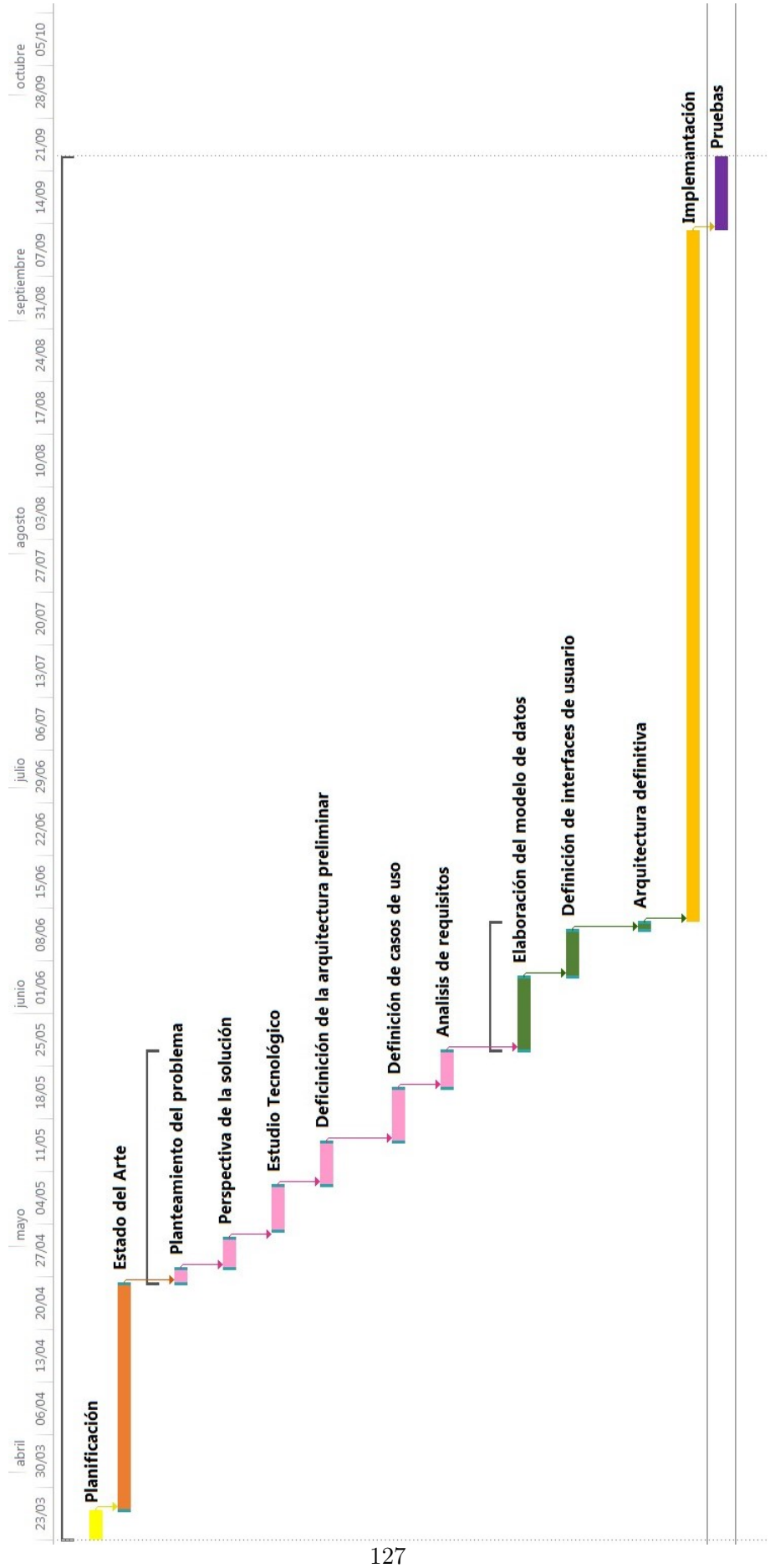


Figura B.1: Diagrama de Gantt de la planificación inicial.

B.0.3. Desarrollo real del proyecto

En este apartado mostramos el desarrollo real del proyecto para después compararlo con la planificación inicial y poder estudiar las desviaciones que se han producido a los largo del proyecto.

En la planificación real se puede observar que el reparto de tiempos es bastante parecido al estimado, aunque si es cierto que en algunas tareas se ha incrementado. El desarrollo del proyecto ha tenido una duración de 811 horas a lo largo de XXX días, siendo la estimación inicial de 724 horas.

Tabla B.2: Planificación real del proyecto.

Nombre	Horas	Fecha Inicio	Fecha Fin
Proyecto	835	23/03/2015	18/10/2015
Planificación	10	23/03/2015	26/03/2015
Estado del Arte	140	26/03/2015	02/05/2015
Análisis	140	02/05/2015	02/06/2015
Planteamiento del problema	6	02/05/2015	02/05/2015
Perspectiva de la solución	20	03/05/2015	07/05/2015
Estudio tecnológico	28	08/05/2015	13/05/2015
Definición de la arquitectura preliminar	27	14/05/2015	20/05/2015
Definición de casos de uso	34	20/05/2015	28/05/2015
Análisis de requisitos	25	28/05/2015	02/06/2015
Diseño	85	02/06/2015	02/06/2015
Elaboración del modelo de datos	40	02/06/2015	13/06/2015
Definición de interfaces de usuario	32	13/06/2015	20/06/2015
Arquitectura definitiva	13	20/06/2015	21/06/2015
Implementación	400	22/06/2015	04/10/2015
Pruebas	60	04/10/2015	18/10/2015

La desviación entre la planificación inicial y la real es la siguiente:

Tabla B.3: Desviación del proyecto.

Nombre	Horas Planificadas	Horas Reales	Diferencia de horas	Desviación %
Proyecto	724	835	111	15,33
Planificación	10	10	0	0,00
Estado del Arte	120	140	0	0,00
Análisis	130	140	14	10,77
Planteamiento del problema	6	6	0	0,00
Perspectiva de la solución	20	20	0	0,00
Estudio tecnológico	25	28	3	12,00
Definición de la arquitectura prelimina	24	27	3	12,50
Definición de casos de uso	30	34	4	13,33
Análisis de requisitos	25	25	0	0,00
Diseño	74	85	11	14,86
Elaboración del modelo de datos	35	40	5	14,28
Definición de interfaces de usuario	30	32	2	6,67
Arquitectura definitiva	9	13	4	44,44
Implementación	350	400	50	14,28
Pruebas	40	60	20	50,00

Como se puede observar en la tabla la desviación del proyecto es de un 15,33 %. Siendo la tarea con mayor desviación fueron las de las pruebas y la arquitectura definitiva. Esto fue así por la necesidad de dividir la aplicación inicial en dos, una para la PKI en sí y otra que se ejecutará en el cliente. También en cuanto a las pruebas necesarias para la realización debido al desconocimiento de las tecnologías utilizadas en el proyecto.

A continuación mostramos la figura con el Diagrama de Gantt con la planificación real.

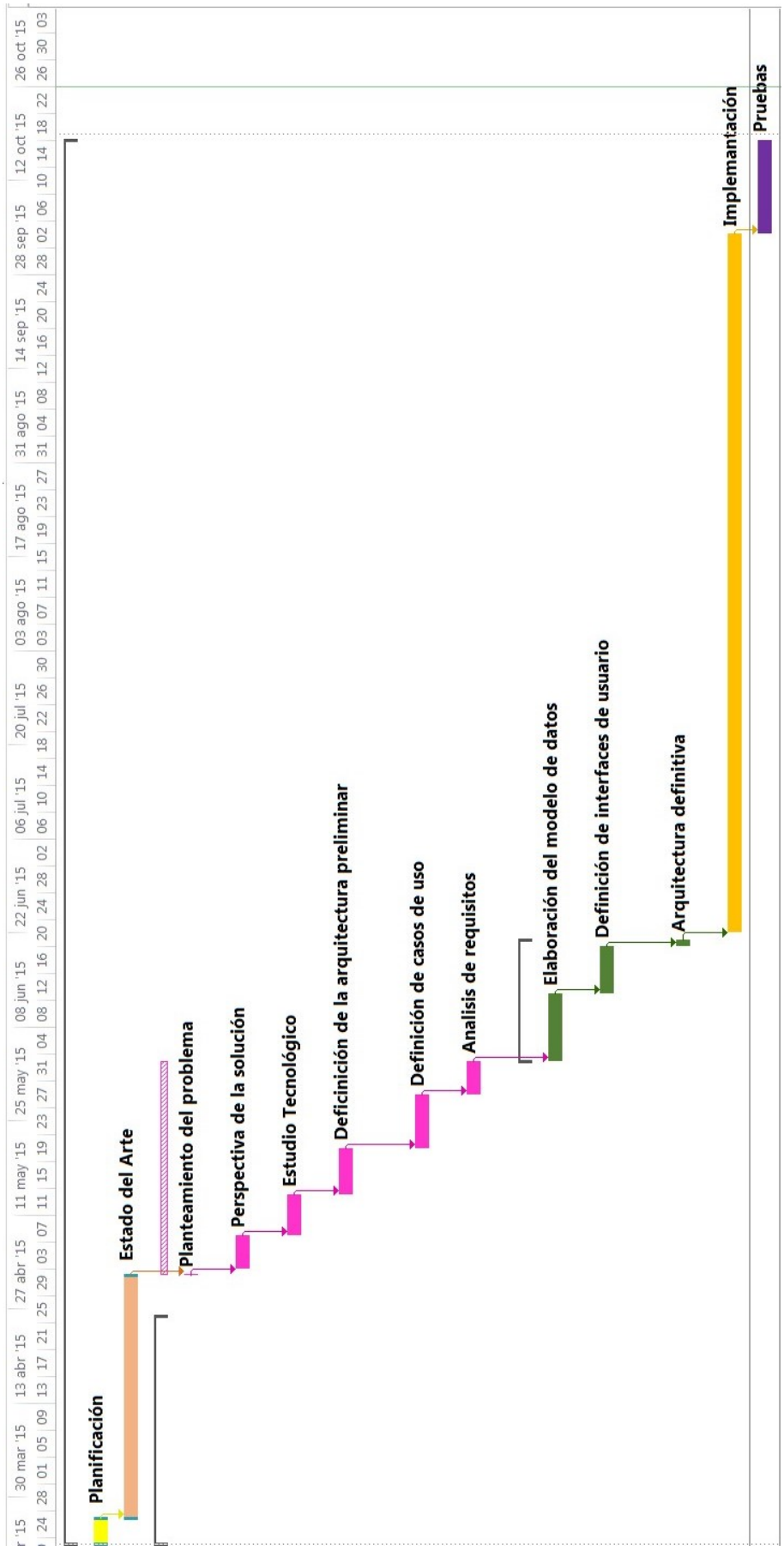


Figura B.2: Diagrama de Gantt de la planificación real

B.0.4. Medios técnicos empleados para el proyecto

En este apartado mostramos las herramientas que se han utilizado para el desarrollo del proyecto. La siguiente tabla muestra estas herramientas con una breve descripción de cada uno de ellas.

Tabla B.4: Medio técnicos utilizados

Herramienta	Descripción
Sistema Operativo Windows 7 Enterprise	**Sistema operativo utilizado para la realización del proyecto**
Microsoft Office 2010	**Aplicaciones del paquete Office utilizadas para la realización del proyecto.**
MicrosoftProyect2013	**Aplicación utilizada para realizar la planificación del proyecto.**
Microsoft Visual Studio 2010 Ultimate	**Aplicación utilizada para la realización del proyecto.**
Notepad++	**Editor de texto utilizado para la realización del proyecto.**
MySql	**Gestor de base de datos utilizado para la realización del proyecto.**
MySQLWorkbench	**Herramienta para el diseño de la base de datos**
Ordenador portátil Dell Latitude E6530	**Ordenador portátil utilizado para la realización del proyecto.**
Disco Duro externo 2TB WD	**Disco duro utilizado para la realización del proyecto.**

B.0.5. Análisis económico del proyecto

En este apartado vamos a realizar el análisis económico del proyecto. En primer lugar indicaremos la metodología utilizada y a continuación se detalla el presupuesto inicial detallado, al igual que el coste real del proyecto una vez concluido.

Como observación indicamos que todas las operaciones están realizadas con una aproximación de dos dígitos decimales.

B.0.6. Metodología de estimación de costes

El presupuesto del proyecto se puede dividir en dos partes, los costes directos y los costes indirectos:

- Por costes indirectos nos referimos a aquellos elementos que están directamente implicados en el desarrollo del proyecto, como por ejemplo los recursos humanos, los

equipos informáticos, el material fungible, el software, los viajes y las dietas cuando se puedan aplicar.

- Por costes indirectos nos referimos a aquellos gastos que se incurren necesariamente para el desarrollo del proyecto, pero que no tienen una relación directa con el desarrollo del mismo. Aquí estaría incluido el consumo eléctrico, el coste del inmueble en el que se realiza el proyecto y el coste de la conexión a internet. Para este proyecto, y de acuerdo con la plantilla proporcionada en la web de la universidad, los costos indirectos se han calculado como un 20 % de los costes directos.

B.0.7. Presupuesto inicial

En este apartado indicamos el presupuesto inicial donde se detallan los costes presupuestados para el proyecto junto con el presupuesto total estimado.

El 21 % de IVA no está aplicado en ninguno de los gastos detallados en esta sección excepto en el coste total del proyecto en el que se indica expresamente que se ha contemplado el IVA para su cálculo.

B.0.8. Gastos de personal

En esta sección indicamos los gastos del personal del proyecto. Hemos utilizado para ello un único ingeniero con una dedicación de 3 horas diarias y de 16 horas durante los fines de semana y festivos durante las 724 horas estimadas para la realización del mismo.

Suponiendo que el coste de la hora del ingeniero sea de 5€ el coste total será:

Tabla B.5: Gastos de personal

Puesto	Coste/Hora	Total Horas	Coste Total
Francisco Javier Castro Martínez (Ing.Técnico)	**5**	**724**	**3620**

B.0.9. Gastos de equipos

En esta sección detallamos los gastos relacionados con los equipos utilizados para la realización del proyecto. Dichos equipos es un ordenador portátil y en la tabla mostramos los costes imputables a ese equipo.

El coste del equipo es el precio de venta al público sin IVA y el de depreciación es el utilizado en el ámbito de la Administración General.

Tabla B.6: Gastos de equipos

Descripción	Coste €	% Uso dedicado al proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable (€)
Ordenador portátil Dell	900	100	6	48	112,50
Disco duro externo WD	85	100	6	48	10,62
				TOTAL	123,12

B.0.10. Gastos de software

En esta sección mostramos los gastos relativos al software utilizado en la realización del proyecto. Los precios no incluyen IVA. Como el software utilizado no se puede comprar debido a que ya está obsoleto lo estimamos con el precio de la versión actual.

Tabla B.7: Gastos de software

Descripción	Coste €	% Uso dedicado al proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable (€)
Sistema Operativo Windows 7 Enterprise	285,00	100	6	36	47,50
Microsoft Office 2010	350	100	6	36	58,33
Microsoft Proyect 2013	Versión Evaluación	100	6	36	00,00
Microsoft Visual Studio 2010 Ultimate	2500	100	6	36	416,66
Notepad ++	Gratuito	100	6	36	0,00
MySql	Gratuito	100	6	36	0,00
MySQL Workbench	Gratuito	100	6	36	000
				TOTAL	522,69

B.0.11. Gastos de material fungible

En esta sección indicamos los gastos en los que se ha incurrido en concepto de consumibles. Aquí estaría incluido el material de oficina como bolígrafos, cuadernos, folios, rotuladores, etc. Tampoco está incluido el IVA.

Tabla B.8: Gastos de material fungible

Descripción	Coste (€)	Cantidad	Coste imputable (€)
Material de Oficina	30	1	30
		TOTAL	30

Tabla B.9: Gastos de material fungible

B.0.12. Gastos de viajes y dietas

Gastos de viajes y dietas
No procede a aplicar este concepto.

B.0.13. Costes directos

En este apartado indicamos los costes directos aplicables al proyecto y que está formado por la suma de los conceptos calculado en los puntos anteriores, es decir, gastos de personal, gastos de equipos, gastos de software, gastos de consumibles y gastos de viajes y dietas.

Tabla B.10: Costos Directos

Descripción	Coste (€)
Gastos de personal	3620
Gastos de equipos	123,12
Gastos de software	522,69
Gastos consumibles	30
Gastos de viajes y dietas	0,00
	4295,81

B.0.14. Costes indirectos

Como hemos dicho anteriormente los costes indirectos se calculan a partir de los costes directos como un 20 % de éstos.

Por tanto los costes indirectos ascienden a 20 % de 4295.81 = **859,16 €**

B.0.15. Estimación de costes

La estimación de costes se realiza a partir de los cálculos realizados en los apartados anteriores. Después de sumar todos los costes aplicamos el IVA, obteniéndose como resultado el total de los costes aplicables al proyecto

Tabla B.11: Estimación de costes

Descripción	Coste (€)
Gastos de personal	**3620**
Gastos de equipos	**123,12**
Gastos de software	**522,69**
Gastos consumibles	**30**
Gastos de viajes y dietas	**0,00**
Costos directos	**4295,81**
Costos indirectos	**859,16**
Total costes sin IVA	**5154,84**
IVA (21 %)	**1082,84**
Total	**6237,81**

B.0.16. Presupuesto para el cliente

El presupuesto para el cliente estará formado por la suma de los costes directos e indirectos sumándole un porcentaje de riesgo para hacer frente a posibles imprevistos surgidos durante el proyecto. También incluimos los beneficios esperados cuyo valor se calcula como un porcentaje del coste total incluyendo el riesgo.

Hemos optado elegir como porcentaje de riesgo un 15 % y un 20 % como beneficio por el desarrollo de la solución. Quedado por tanto el presupuesto como sigue:

Tabla B.12: Presupuesto para el cliente

Descripción	Coste (€)
Gastos de personal	3620
Gastos de equipos	123,12
Gastos de software	522,69
Gastos consumibles	30
Gastos de viajes y dietas	0,00
Costos directos	4295,81
Costos indirectos	859,16
Total costes sin riesgo	5154,84
Riesgos(15 %)	859,16
Total costes sin beneficios	5928,21
Beneficios (20 %)	1185,64
Total costes sin IVA	7113,85
IVA (21 %)	1493,90
Total	8607,75